PCSIC
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

PCSIC
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA - EXTERNA

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA GRUPO LAVORO			
MÊS / ANO	VERSÃO	CONFIDÊNCIALIDADE	DESCRIÇÃO
Agosto 2023	Versão 1.6 COMPLETA	Documento Público	Nº POL-SEG-001
Março 2024	Versão 1.7 Completa	Documento Publico	Nº POL-SEG-001
Setembro 2024	Versão 1.8 Completa	Documento Publico	Nº POL-SEG-001

Sumário

1 INTRODUÇÃO

A Política Corporativa de Segurança da Informação e Cibernética é mantida e divulgada pelo Grupo Lavoro Agro Holding ("Grupo Lavoro") para orientar seus colaboradores e prestadores de serviços sobre como proteger adequadamente as informações manipuladas no exercício de suas funções. Todas as informações do Grupo Lavoro, de seus clientes, colaboradores, prestadores de serviços, acionistas e demais partes interessadas devem ser obtidas, manipuladas, armazenadas e, eventualmente, destruídas conforme as determinações desta política.
As determinações aqui contidas refletem a visão, a missão e os valores do Grupo Lavoro, bem como o comprometimento do Comitê Executivo de Segurança da Informação e Privacidade de Dados com a proteção das informações da empresa ou sob sua guarda, conforme as determinações da legislação brasileira e as melhores práticas de mercado.

2 OBJETIVOS

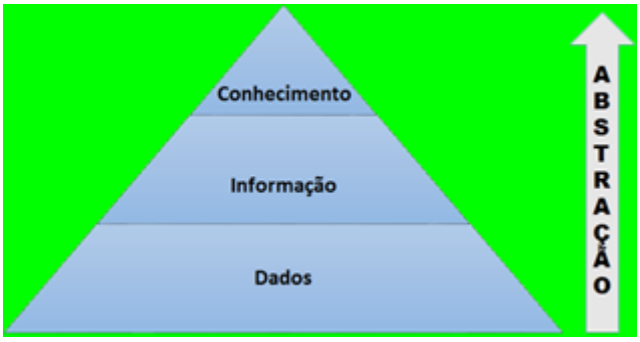
Objetivo Geral:

Auxiliar na missão e visão da organização, bem como aplicar os valores e assegurar o cumprimento dos requisitos legais e de imagem da companhia quanto a Segurança da Informação e Cibernética.

Objetivos Específicos:

- Garantir aplicabilidade da própria política de segurança a todos os colaboradores, parceiros, prestadores, visitantes ou quaisquer outros agentes em contato com informações da companhia;
- Manter informações sensíveis, em especial informações confidenciais de clientes, sob sigilo necessário e exigido pelos contratos de confidencialidade estabelecidos;
- Aplicar a cultura de segurança da informação para todos os colaboradores e terceiros, fornecendo através das suas normas e procedimentos acessórios conhecimento suficiente para reconhecer e evitar ataques cibernéticos;
- Melhorar de maneira contínua a segurança da informação dentro da companhia.

3 TERMOS E DEFINIÇÕES



A segurança da informação tem como base alguns princípios fundamentais abaixo descritos:

Dado: Não possui significado relevante e não conduz a nenhuma compreensão. Representa algo que não possui sentido em isolado.

Informação: Conjunto organizado de dados para formação de compreensão em um contexto.

Confidencialidade: É a capacidade de se manter guardado um dado ou informação e disponível apenas a quem se deva possuir acesso. A senha de acesso à conta bancária pessoal é uma informação que deve ser confidencial (acessível apenas ao correntista).

Integridade: É a capacidade de se garantir que um dado ou informação não foi adulterada sem que seja percebida. Ex.: ao modificar um documento, o aplicativo que abre o documento, mostrar que foi alterado por fulano.

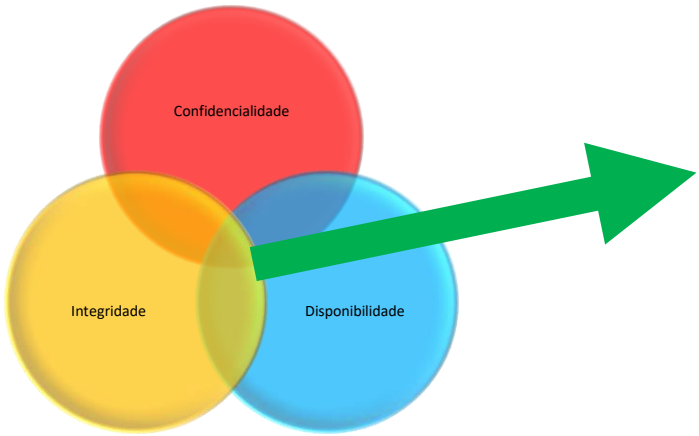
Disponibilidade: É a característica em tornar acessível o dado ou informação a quem seja possuidor de seu acesso quando necessário.

Não Repúdio: Capacidade que garante a autoria de um dado ou informação, não podendo este recusar (repudiar) a autoria.

Dono da informação: É a representação de alguém que possui a propriedade e direito sobre o dado ou informação. Em muitas vezes o dono da informação é a própria companhia, sendo então o colaborador ou terceiro custodiante.

Custodiante: É a representação de alguém que possui a responsabilidade de manipulação do dado ou informação em determinado momento. Ex.: colaborador que é responsável por atualizar cadastro de clientes. No momento em que possui acesso aos dados e informações torna-se custodiante e responsável pela manutenção da CID (confidencialidade, integridade e disponibilidade), bem como pelas sanções porventura aplicáveis em caso de descumprimento.

Segurança da Informação: Engloba a garantia dos conceitos de confidencialidade, integridade, disponibilidade e outros (como não repúdio) tanto para dados, quanto para informação.



BASE DA SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais bens da instituição. Assim, o Grupo Lavoro define a estratégia corporativa de segurança da Informação e cibernética para proteger a integridade, disponibilidade e confidencialidade da informação.
Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro digital do Grupo Lavoro.
Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde a coleta até o descarte.

4 RESPONSABILIDADES

Todos os colaboradores e terceiros a que esta política é aplicável, são responsáveis pela aplicação e manutenção da segurança da informação na companhia.

- **Responsabilidades comuns a todos (inclusive colaboradores, terceiros e visitantes):**
  - Aplicar todos os itens contidos nesta política e demais documentos auxiliares;
  - Zelar pela informação e recursos da companhia;
  - Reportar incidentes de segurança pelos meios corretos.;
- **Alta direção:** Apoiar este documento, bem como quaisquer iniciativas apreciadas pelo Comitê de Segurança da Informação e Privacidade de Dados ou por qualquer outro grupo ou indivíduo para o objetivo da aplicação da presente política de segurança.
- **Comitê de Segurança da Informação e Privacidade de Dados / Tecnologia da Informação:**
  - Estabelecer e manter um Sistema de Gestão de Segurança da Informação, sob o qual está apoiada esta Política de Segurança;
  - Auxiliar na definição e operação dos controles necessários para o cumprimento desta política de segurança da informação. Ex.: firewall, antivírus, credenciais de acesso, criptografia, etc;
  - Apreciar assuntos relevantes à companhia no quesito Segurança da Informação e normatizar as tratativas adequadas;

5 ABRANGÊNCIA EM SISTEMAS E ATIVOS COMPUTACIONAIS

As premissas definidas em política são aplicáveis a todos os ambientes computacionais de processamento de dados do Grupo Lavoro, estendendo, mas não se limitando a todos os serviços e sistemas em cloud, bases de dados, sistemas operacionais, hardware, software, dispositivos de redes, telefonia, dispositivos móveis, além de ambientes de terceiros que de forma física ou lógica estejam integrados ou conectados nos ambientes do Grupo Lavoro e seu parque tecnológico.
O Grupo Lavoro pauta suas ações em boas práticas do mercado nacional e internacional, são elas:

- ISO 27701 – Gestão da segurança da Informação;
- ISO 27002 – Políticas para segurança da informação;
- NIST – Cyber Security Framework;
- CIS – Center for Internet Security;

6 DIRETRIZES

A Política de Segurança da informação deve estar disponível em local acessível aos colaboradores e protegidas contra alterações.
A Política de Segurança da Informação é revisada anualmente pela área de Segurança do Grupo Lavoro com aplicação no Brasil e no exterior.
A inclusão de diretrizes ou exceções por requisito regulatório e a publicação nas unidades do exterior, serão identificadas pelo responsável por segurança da informação da unidade, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pelo Comite de Segurança da Informação e Privacidade de Dados.
A adesão à essa Política e eventuais desvios, no Brasil e nas unidades no exterior, são reportados periodicamente pelo Comite de Segurança da Informação e Privacidade de Dados.

7 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O Grupo Lavoro tem por política respeitar a privacidade e segurança dos dados pessoais a que tem acesso. Em seus processos estabelecidos, o Grupo Lavoro procura certificar-se que o tratamento dos dados pessoais se dará de forma transparente, não sendo realizado para finalidades distintas ou incompatíveis aquelas que fundamentaram sua coleta

Todos os dados e informações compartilhados pelos visitantes, clientes, colaboradores e parceiros nos sites e aplicativos do Grupo Lavoro serão recebidas por colaboradores da empresa e tratados como confidenciais, de modo que não serão divulgados a terceiros, de forma gratuita ou onerosa, ou de qualquer maneira expostos sem prévio consentimento, salvo mediante aos termos do art. 7º da Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709/2018.

8 MANUTENÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação deve ser revisada a cada 12 meses. O Comitê de Segurança da Informação pode, no entanto, iniciar o processo de revisão a qualquer momento.

9 POLÍTICAS – NORMAS – PROCEDIMENTOS ESPECÍFICOS

A Política de Segurança da Informação é composta por além de suas diretrizes das seguintes normas e procedimentos:

- Norma de Classificação de Informações;
- Procedimento de Controle de Acesso e Autenticação
- Procedimento de Operações e Gerência de Sistemas
- Política de Gestão de Incidentes Cibernéticos
- Política de Gestão de Vulnerabilidades

10 CUMPRIMENTO DAS NORMAS

É responsabilidade de todo colaborador ou prestador de serviço, zelar pelo cumprimento da Política de Segurança da Informação do Grupo Lavoro. Nos casos de conhecimento de desvios da Política, possíveis incidentes de cibersegurança, vazamento de informações que afetem a confidencialidade ou outras normas da Segurança da Informação e Cibernética, os colaboradores e terceiros são incentivados a relatar ao canal oficial da área de Segurança da Informação da Lavoro pelo e-mail security@lavoroagro.com para que ações preventivas e corretivas possam ser tomadas. Em casos de incidentes de segurança a área de TI, se necessário, poderá notificar os colaboradores ou prestadores de serviço quanto ao descumprimento das normas de segurança da informação.

10.1 CANAIS DE COMUNICAÇÃO

- security@lavoroagro.com

11 APROVAÇÃO

VERSÃO	DATA	REVISÃO	RESPONSÁVEL
1.8	06/09/2024	Revisão total da PCSIC onde foram extraidas Normas e Procedimentos, criando-se documentos acessórios tornando a PCSIC documento unico.	Antonio Sobrinho
1.7	26/03/2024	Revisado padrão de expiração de senhas e numero de tentativas para bloqueio	Antonio Sobrinho
1.6	31/08/2023	Revisado LGPD e Acessos Privilegiados	Antonio Sobrinho
1.5	27/12/2022	Ajustes, revisão e envio para aprovação	Fernando Cesar de Oliveira
1.4	01/06/2021	Ajustes, revisão e envio para aprovação	Fernando Cesar de Oliveira
1.3	26/05/2021	Ajustes, revisão e envio para aprovação	Fernando Cesar de Oliveira
1.2	26/04/2021	Ajustes	Thiago Mendes da Silva
1.1	16/09/2020	Revisão e alteração	Thiago Mendes da Silva
1.0	02/09/2020	Emissão Inicial	Hubert Thomaz