Grupo Lavoro Agro Holding S.A.

Política Corporativa de Segurança da Informação e Cibernética - PCSIC

Editado em junho/2021

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA GRUPO LAVORO AGRO HOLDING

MÊS / ANO	VERSÃO	CONFIDENCIALIDADE	DESCRIÇÃO
Junho 2021	Versão 1.0 SIMPLIFICADA	Documento Público	Nº POL-SEG-001

1. PREMISSAS

1.1. Os pilares da política de Segurança da Informação e Cibernética do **Grupo Lavoro Agro Holding** estão aderentes aos valores da Instituição e presentes no cumprimento da função de todos os colaboradores.

1.2. As suas premissas são:

- Proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados;

- Garantir a continuidade do processamento das informações críticas ao negócio;

- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual e atender às leis e normas que regulamentam as atividades do **Grupo Lavoro Agro Holding** em seu mercado de atuação;

- Determinar os mecanismos de gestão de riscos cibernéticos.

2. OBJETIVO

2.1. Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

3. PÚBLICO-ALVO

3.1. As áreas de SEGURANÇA DA INFORMAÇÃO E DE GOVERNANÇA DE DADOS são responsáveis por manter, atualizar e divulgar a Política Corporativa de Segurança da Informação e Cibernética, as normas e procedimentos que dela derivam.

3.2. Esta Política aplica-se a todos os administradores, colaboradores, terceiros e demais envolvidos nas atividades do **Grupo Lavoro Agro Holding** e suas empresas ou entidades controladas no Brasil e no exterior.

4. INTRODUÇÃO

4.1. A informação é um dos principais bens da instituição. Assim, o **Grupo Lavoro Agro Holding** define a estratégia corporativa de segurança da Informação e cibernética para proteger a integridade, disponibilidade e confidencialidade da informação.

4.2. 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 Agro Holding**.

4.3. 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.

5. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

5.1. A nossa visão sobre Segurança da Informação e Cibernética está baseada nos seguintes princípios:

•**Confidencialidade** - Somente o Usuário da Informação, que esteja devidamente autorizado pelo Gestor da Informação, deve ter acesso às Informações respeitando os critérios de segregação de funções pré-definidos;

•**Integridade** - Garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo Gestor da Informação;

•**Disponibilidade** - Deve garantir que as Informações estejam sempre disponíveis para o Usuário da Informação;

•**Autenticidade** - Garante a identidade de quem está enviando a Informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem (irretratabilidade).

6. ABRANGÊNCIA EM SISTEMAS E ATIVOS COMPUTACIONAIS

6.1. As premissas definidas em política são aplicáveis a todos os ambientes computacionais de processamento de dados do **Grupo Lavoro Agro Holding**, estendendo, mas não se limitando a todos os servidores, 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 Agro Holding** e seu parque tecnológico.

6.2. O **Grupo Lavoro Agro Holding** pauta suas ações em boas práticas do mercado nacional e internacional, são elas:

•ISO 27002 – Políticas para segurança da informação;
•ISO 27701 – Gestão da Privacidade da Informação;
•NIST – Cyber Security Framework;
•NIST – Privacy Framework;

•CIS – Center for Internet Security.

7. DIRETRIZES

7.1. Todas as políticas de segurança da informação devem estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

7.2. As políticas de segurança da informação são revisadas anualmente pelo **Grupo Lavoro Agro Holding** com aplicação no Brasil e no exterior.

7.3. 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 Comitê de Segurança da Informação.

7.4. A adesão à essa Política e eventuais desvios, no Brasil e nas unidades no exterior, são reportados periodicamente pela Comitê de Segurança da Informação e demais comitês de risco. A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente.

7.5. As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

8. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

8.1. Para assegurar que as informações tratadas estejam adequadamente protegidas, o **Grupo Lavoro Agro Holding** adota os seguintes processos:

8.1.1. **Gestão de Ativos** - Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação e autorização).

Os ativos do **Grupo Lavoro Agro Holding**, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

8.1.2. **Classificação da Informação -** As informações devem ser classificadas de acordo com a confidencialidade, conforme descrito em documentos internos.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

8.1.3. **Gestão de Acessos -** As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos do **Grupo Lavoro Agro Holding**.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

8.1.4. **Gestão de Riscos** - Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre

os ativos do **Grupo Lavoro Agro Holding**, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura do **Grupo Lavoro Agro Holding**, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

8.1.5. **Gestão de Riscos em Prestadores de Serviços e Parceiros** - Os prestadores de serviços e parceiros contratados pelo **Grupo Lavoro Agro Holding** devem ser classificados considerando alguns critérios, conforme documentos internos.

Dependendo da classificação, o prestador de serviços ou parceiro passará por avaliação de risco, que pode incluir a validação in loco dos controles de SI, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Os prestadores de serviços e parceiros devem informar os incidentes relevantes (conforme definido no item 8.1.6. deste documento), relacionados às informações do **Grupo Lavoro Agro Holding** armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

8.1.6. **Tratamento de Incidentes de Segurança da Informação e Cyber Security** - A área de Cyber Security monitora a segurança do ambiente tecnológico do **Grupo Lavoro Agro Holding** no Brasil, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo **Grupo Lavoro Agro Holding**. Para o seu grau de relevância serão considerados aspectos como impacto na continuidade dos negócios ou comprometimento de dados de clientes e do público em geral. Incidentes classificados como relevantes devem ser comunicados ao Regulador, ao titular do dado, e ao Comitê de Privacidade de Dados e Segurança da Informação, quando envolverem dados pessoais que possam acarretar risco ou causar dano relevante aos titulares.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, etc.

Informações sobre incidentes que possam impactar outras instituições financeiras no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

No exterior, a gestão de incidentes de segurança da informação e cibernéticos é realizada por cada Unidade Internacional que deve reportá-los tempestivamente ao Comitê de Segurança da Informação no Brasil.

A área de Riscos elaborará Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Risco, conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, o **Grupo Lavoro Agro Holding** realiza testes de continuidade de negócios simulando cenários de incidentes críticos de Cyber Security, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

8.1.7. **Conscientização em Segurança da Informação e Cyber Security** - O **Grupo Lavoro Agro Holding** promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, plataformas de ensino digital (e-learning / UniLavoro), mídias eletrônicas ou redes sociais aos colaboradores e clientes.

8.1.8. **Governança com as Áreas de Negócio e Tecnologia** - As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de segurança da informação.

8.1.9. **Segurança Física do Ambiente** - O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes, conforme descrito nos documentos internos.

8.1.10. **Segurança no Desenvolvimento de Sistemas de Aplicação -** O processo de desenvolvimento de sistemas deve garantir a aderência aos documentos internos e boas práticas de segurança da instituição.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

8.1.11. **Gravação de Logs** - É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados.

8.1.12. **Programa de Cyber Security** - O Programa de Cyber Security do **Grupo Lavoro Agro Holding** é norteado pelos seguintes princípios:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição;
- Assessments externos de Consultorias Especializadas.

Conforme sua criticidade, as ações do programa dividem-se em:

- **Críticas**: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;

• **Sustentação**: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

• **Estruturantes**: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o Grupo para o futuro.

8.1.13. **Proteção de perímetro** - Para proteção da infraestrutura do **Grupo Lavoro Agro Holding** contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de DDoS, Spam, Phishing, APT/Malware, invasão de dispositivos de rede e servidores, ataques a aplicação e scanners de portas externas.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares não gerenciados ou não homologados.

8.1.14. **Governança com as Unidades Internacionais** - As unidades internacionais devem possuir um responsável por segurança da informação, independente das áreas de negócio e tecnologia, que se reporta matricialmente ao Comitê de Segurança da Informação.

9. PROPRIEDADE INTELECTUAL

9.1. A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

9.2. Pertencem exclusivamente ao **Grupo Lavoro Agro Holding** todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelo colaborador ao **Grupo Lavoro Agro Holding** na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja

propriedade intelectual pertença ao **Grupo Lavoro Agro Holding**, ou tenham sido por ele disponibilizado, inclusive informações e conteúdo que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa do **Grupo Lavoro Agro Holding**.

9.3. É dever de todos os colaboradores zelar pela proteção da propriedade intelectual do **Grupo Lavoro Agro Holding**.

10. DECLARAÇÃO DE RESPONSABILIDADE

10.1. Periodicamente os colaboradores do **Grupo Lavoro Agro Holding** devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Privacidade de Dados e Segurança da Informação.

10.2. Os contratos firmados com o **Grupo Lavoro Agro Holding** devem possuir cláusula que assegure a confidencialidade das informações e a obrigatoriedade de seguir as regulamentações vigentes, referentes ao tema de privacidade de dados e segurança da informação.

11. PAPÉIS E RESPONSABILIDADES

11.1. As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas no Brasil e no exterior pelo Comitê de Segurança da Informação e discutidos nos temas específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou de Tecnologia.

11.1.1. **Compliance** - Os papéis e responsabilidades de Compliance Interna estão descritos em política interna.

11.1.2. **Controles Internos** - Os papéis e responsabilidades de Controles Internos estão descritos em política interna.

11.1.3. **Segurança de Tecnologia da Informação** - Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;

• Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;

• Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI).

• Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê de Segurança da Informação.

• Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.

• Estabelecer e disseminar uma cultura de segurança da informação.

• Propor o investimento para a segurança da informação para atender aos objetivos desta política.

• Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.

• Definir padrões mínimos de segurança para as Unidades Internacionais e Empresas controladas no Brasil e no exterior e Entidades mantidas ou geridas pelo **Grupo Lavoro Agro Holding**, garantindo alinhamento com os objetivos de segurança da informação definidos pelo **Grupo Lavoro Agro Holding**.

11.1.4. **Unidades Internacionais** - Atuar proativamente na identificação, prevenção e correção dos riscos e reportar periodicamente ao Departamento de Segurança de Tecnologia da Informação.

11.1.5. **Empresas e Entidades do Grupo Lavoro Agro Holding** - Empresas do grupo controladas no Brasil e no exterior e entidades mantidas ou geridas pelo **Grupo Lavoro Agro Holding** devem avaliar as diretrizes e requisitos estabelecidos nesta política e em seus anexos, reportando periodicamente ao Departamento de Segurança de Tecnologia da Informação os riscos identificados, adequando seus procedimentos de segurança internos conforme seu segmento de negócio. Estas empresas devem seguir modelo de governança definido pelo Departamento de Segurança da Tecnologia da Informação.

11.1.6. **Comitê de Privacidade de Dados e Segurança da Informação** - Aprovar a estratégia, objetivos e ações necessárias para a mitigação dos riscos dos processos de privacidade de dados e segurança da informação.

11.1.7. **Comitê de Riscos -** Supervisionar a estratégia de gestão dos riscos, seus respectivos processos e controles internos, bem como acompanhar os projetos de privacidade de dados e segurança da informação e cibernética do **Grupo Lavoro Agro Holding**.

11.1.8. **Área de Tecnologia** - Manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

11.1.9. **Área de Negócio** - Proteger as informações do **Grupo Lavoro Agro Holding** sob sua responsabilidade.

12. SANÇÕES DISCIPLINARES

12.1. As violações a esta política estão sujeitas às sanções disciplinares previstas em política interna, bem como nas normas internas das empresas do **Grupo Lavoro Agro Holding** e na legislação vigente onde as empresas estiverem localizadas.

13. DOCUMENTOS RELACIONADOS

13.1. Esta Política Externa de Segurança da Informação é complementada por procedimentos específicos de Segurança em conformidade com os aspectos legais e regulamentares, e pela Política Interna de Segurança da Informação e Política de Privacidade de Dados.

14. VIOLAÇÕES E PENALIDADES

14.1. Na ocorrência de infrações relacionadas com esta Política ou qualquer documento do Programa de Integridade do **Grupo Lavoro Agro Holding**, o Terceiro ou o Colaborador estará sujeito às medidas disciplinares previstas na Política de Gestão de Consequências do **Grupo Lavoro Agro Holding** e/ou normas legais aplicáveis.

15. CONFLITOS, EXCEÇÕES E ESCLARECIMENTOS

15.1. Qualquer exceção ao determinado nesta Política deverá ser requerida mediante o envio de solicitação endereçada ao **Comitê de Privacidade de Dados e Segurança da Informação** do **Grupo Lavoro Agro Holding** com a descrição do requerimento, justificativas e critérios utilizados para o pedido.

15.2. Nenhuma exceção poderá ser realizada em desacordo com o Programa de Integridade, a legislação vigente e sem aprovação prévia e escrita do Conselho de Administração, que votará com base no parecer apresentado pelo **Comitê de Privacidade de Dados e Segurança da Informação**.

15.3. Quaisquer dúvidas e conflitos detectados com outras normas deverão ser encaminhados ao Canal de Transparência para os esclarecimentos necessários.

16. CANAL DE TRANSPARÊNCIA

16.1. O **Grupo Lavoro Agro Holding** incentiva todos os seus Colaboradores e Terceiros a denunciarem quando suspeitarem ou detectarem violações.

16.2. Todos que se relacionam com o **Grupo Lavoro Agro Holding** devem comunicar as violações ou possíveis violações às diretrizes desta Políticas e demais regras estabelecidas pelo Programa de Integridade do **Grupo Lavoro Agro Holding**, por meio do Canal de Transparência, acessível em:

https://contatoseguro.com.br/lavoro

16.3. Os relatos poderão ser realizados pelo denunciante de forma anônima, caso este prefira não se identificar.

16.4. Todas as situações reportadas serão avaliadas e as devidas tratativas conduzidas dentro do mais estrito sigilo, justiça, profundidade, tempestividade, respeito e razoabilidade, sendo permitido o apoio técnico especializado externo.

VERSÃO	DATA	REVISÃO	RESPONSÁVEL
1.2	07/06/2021	Revisão e alteração	Elvis Adriano Machado
1.1	02/06/2021	Revisão e alteração	Hubert Thomaz
1.0	26/05/2021	Emissão Inicial	Fernando Cesar de Oliveira