POL-01
PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aprovação:

Elaborado:	Maycon Gabriel Ferreira Da Silva
Aprovado:	Sheila Ariana Xavier Valencio
Data:	05/01/2026
Versão:	1.0

1. Objetivo

A Política de Segurança da Informação estabelece os princípios e diretrizes que orientam a proteção das informações tratadas pela Fitovision, assegurando sua confidencialidade, integridade, disponibilidade e conformidade com requisitos legais, contratuais e operacionais. A política reflete o compromisso institucional com a prevenção de incidentes, a continuidade das operações e a promoção de um ambiente seguro e responsável no uso de ativos e recursos tecnológicos. A presente política está alinhada à norma ISO/IEC 27001:2022, servindo como base para o Sistema de Gestão de Segurança da Informação (SGSI) da Fitovision e orientando a implementação dos controles do Anexo A.

2. Contexto Organizacional

A Fitovision é uma empresa de tecnologia focada no desenvolvimento de soluções SaaS para pesquisa agrícola, incluindo captura, processamento e análise de dados de ensaios, imagens de sensoriamento remoto (NDVI/NDRE) e modelos estatísticos avançados. A operação ocorre em ambiente híbrido, composto por infraestrutura em ambiente hospedado em datacenter de terceiro, serviços em nuvem e colaboradores atuando em regime remoto. O correto tratamento das informações e a disponibilidade dos serviços são essenciais ao negócio e aos clientes.

3. Escopo

Este documento aplica-se a todos os sistemas SaaS, APIs, pipelines de dados, bases de dados, servidores físicos e virtuais, ambientes em nuvem, repositórios Git, endpoints corporativos, e colaboradores internos ou externos que tratem informações da Fitovision.”

4. Princípios de Segurança da Informação

A segurança da informação na Fitovision se baseia nos seguintes princípios:
Confidencialidade: informações acessadas apenas por pessoas autorizadas.
Integridade: informações preservadas contra alteração indevida.
Disponibilidade: informações e serviços acessíveis quando necessários.
Proporcionalidade: controles adequados ao porte, contexto e riscos da organização.
Responsabilidade compartilhada: todos contribuem para um ambiente seguro.

A Fitovision adota uma abordagem baseada em riscos para decisões relacionadas à segurança da informação, assegurando que controles sejam selecionados, implementados e avaliados conforme a probabilidade e impacto dos riscos identificados.

5. Termos e Definições Essenciais

Informação: qualquer dado físico ou digital utilizado em atividades corporativas.
Ativo: equipamento, sistema, processo ou recurso que suporta o uso da informação.
Dispositivo endpoint: dispositivo individual, como notebook ou celular corporativo.
Credencial: senha, token, MFA ou qualquer método de autenticação.
Incidente de segurança: evento que compromete ou possa comprometer a informação.
Classificação da informação: categorização conforme sensibilidade e criticidade.

6. Responsabilidades Institucionais

Alta Direção: Estabelece diretrizes, aprova esta política, apoia o SGSPI e garante recursos adequados.
Gestor do SGSI: Coordena controles, orienta equipes, conduz avaliações e acompanha o tratamento de incidentes.
Área de TI / DevOps: Mantém infraestrutura, serviços e aplicações com padrões de segurança compatíveis com o ambiente da Fitovision.
Demais Áreas e Gestores: Promovem o cumprimento das diretrizes desta política e apoiam a proteção da informação no âmbito de suas atividades.
Terceiros e Prestadores: Respeitam os acordos de confidencialidade e tratam informações conforme requisitos desta política.

– Diretoria de TI: Define diretrizes estratégicas de segurança e aprova políticas.
– Gestor do SGSI: Mantém o Sistema de Gestão de Segurança da Informação, monitora controles, coordena auditorias.
– DPO: Garante conformidade com a LGPD, orienta sobre privacidade e tratamento de dados pessoais.
– Usuários: Proteger credenciais, seguir políticas internas e reportar incidentes de segurança imediatamente.

7. Diretrizes Gerais de Segurança da Informação

As diretrizes a seguir estabelecem o conjunto de regras institucionais para proteção das informações e uso adequado dos ativos da Fitovision.

7.1 Classificação e Tratamento da Informação

A informação é tratada conforme seu grau de sensibilidade e valor para a Fitovision. São adotadas práticas de classificação que orientam seu armazenamento, acesso e compartilhamento, garantindo que dados estratégicos, código-fonte, informações de clientes e informações pessoais recebam proteção proporcional ao risco envolvido. Informações sensíveis são armazenadas exclusivamente em ambientes autorizados, preservadas contra divulgação indevida e compartilhadas apenas quando houver necessidade e autorização apropriada. O descarte de informações ocorre por meios seguros que evitem exposição ou recuperação não autorizada.

7.2 Controle de Acesso e Uso de Credenciais

O acesso a sistemas, aplicações, repositórios e ambientes é concedido com base na necessidade e compatibilidade com as funções exercidas. Credenciais são únicas, individuais e protegidas por mecanismos seguros, incluindo senhas fortes e autenticação multifator quando aplicável. As permissões são revisadas periodicamente e encerradas quando deixarem de ser necessárias. Os ambientes críticos, como repositórios de código e serviços em nuvem, seguem segregação adequada e privilegiam o princípio do menor privilégio.

7.3 Segurança Física e Ambiente de Trabalho (Mesa Limpa e Tela Limpa)

As instalações e os equipamentos que suportam as atividades da Fitovision são protegidos contra acesso físico indevido e exposição acidental de informações. A organização adota práticas de tela limpa e mesa limpa, mantendo documentos guardados, telas bloqueadas durante ausências e evitando que informações fiquem expostas visualmente. Equipamentos são mantidos em locais seguros e protegidos contra riscos ambientais, quedas, perda ou danos.

7.4 Uso Aceitável de Ativos, Dispositivos e Equipamentos

Os ativos disponibilizados pela Fitovision, como sistemas, aplicações, serviços em nuvem, credenciais e recursos de comunicação, são utilizados exclusivamente para suportar atividades corporativas, preservando sua integridade e finalidade. Os dispositivos fornecidos pela organização seguem padrões de configuração segura, mantendo sistemas atualizados, proteção contra malware, bloqueio automático e controle sobre aplicações autorizadas.

Considerando o modelo operacional da Fitovision, que permite o uso de dispositivos pessoais (BYOD) para execução de atividades de trabalho, são adotados cuidados específicos para garantir a proteção da informação independente do tipo de equipamento. Dispositivos pessoais utilizados para fins corporativos seguem parâmetros mínimos de segurança, como proteção por senha ou biometria, bloqueio automático, atualizações regulares, uso de antivírus ou ferramentas equivalentes, e armazenamento das informações corporativas apenas em ambientes autorizados. Informações de clientes, código-fonte, dados analíticos e demais conteúdos sensíveis permanecem exclusivamente em serviços corporativos definidos pela Fitovision, não sendo permitida sua guarda permanente na memória local desses dispositivos.

A instalação de aplicações, bibliotecas ou extensões em dispositivos pessoais ocorre com discernimento e compatibilidade com as atividades exercidas, evitando ferramentas que possam comprometer a segurança das informações tratadas. Sempre que um dispositivo pessoal apresentar falhas, perda, roubo ou suspeita de comprometimento, a Fitovision deve ser informada para que possam ser adotadas as medidas preventivas necessárias, mitigando riscos de exposição de dados corporativos.

7.5 Proteção de Dispositivos Endpoint

Os dispositivos utilizados para acessar informações, sistemas ou serviços da Fitovision são protegidos por medidas que preservam sua confiabilidade e reduzam riscos de comprometimento. Dispositivos corporativos seguem padrões definidos de configuração segura, incluindo mecanismos de autenticação forte, proteção contra malware, criptografia de dados, aplicação de atualizações e bloqueio automático, garantindo operação alinhada aos requisitos de segurança da organização.

No cenário que permite o uso de dispositivos pessoais (BYOD), a proteção da informação ocorre através de controles aplicados tanto nos ambientes corporativos quanto na forma de acesso realizada nesses dispositivos. Os dados corporativos permanecem armazenados exclusivamente em serviços autorizados pela Fitovision, como plataformas em nuvem, repositórios, drives corporativos ou aplicações oficiais, evitando a guarda local em dispositivos pessoais. Os endpoints pessoais utilizados para fins corporativos mantêm configurações mínimas de segurança, como versões atualizadas do sistema operacional, proteção por senha ou biometria,

bloqueio automático, uso de ferramentas de proteção contra malware e acesso por conexões seguras.

A Fitovision adota práticas de monitoramento e prevenção para ambientes sensíveis, restringindo o acesso a dados críticos apenas a dispositivos ou conexões que atendam aos requisitos estabelecidos. Quando um dispositivo pessoal apresentar sinais de comprometimento, falhas, perda ou roubo, a organização deve ser informada prontamente para que sejam tomadas as medidas necessárias de proteção das informações corporativas.
6.6 Segurança de Sistemas, Redes e Comunicação

Os sistemas, redes e serviços utilizados pela Fitovision seguem padrões de segurança compatíveis com o ambiente da organização. São utilizadas redes corporativas ou conexões protegidas, como VPN, sempre que necessário para garantir a proteção das informações transmitidas. A comunicação eletrônica segue canais autorizados, evitando compartilhamento de informações sensíveis por meios inseguros ou informais. Sistemas críticos seguem monitoramento compatível com sua importância e riscos associados.

7.6 Desenvolvimento Seguro e Ciclo de Vida das Aplicações

O desenvolvimento e evolução das aplicações seguem práticas de segurança desde sua concepção, contemplando análise de código, revisão entre pares, uso de repositórios confiáveis e controle de versões. Dependências, bibliotecas e frameworks são atualizados e avaliados quanto à segurança antes de serem incorporados às soluções. Ambientes de desenvolvimento, homologação e produção são segregados e seguem controles independentes. Alterações em aplicações seguem padrões seguros e são testadas antes de sua disponibilização.

7.7 Diretrizes de projeto

Todos os projetos, integrações, novas funcionalidades e evoluções de sistemas da Fitovision devem adotar o princípio de ‘security by design’, incorporando requisitos de segurança desde a concepção até o desenvolvimento, teste, implantação e manutenção. Isto inclui análise prévia de riscos, definição de controles mínimos, tratamento de dados sensíveis, gestão adequada de dependências e validações de segurança antes de liberar alterações para ambientes produtivos.

7.8 Gestão de Vulnerabilidades e Atualizações

A organização identifica e avalia vulnerabilidades técnicas, aplicando correções e melhorias de forma proporcional à sua criticidade. São utilizados mecanismos de análise contínua, varreduras técnicas e acompanhamento de atualizações relevantes para sistemas, dispositivos e componentes utilizados. Vulnerabilidades emergentes são monitoradas com base em fontes confiáveis, permitindo atuação proativa.

7.9 Armazenamento, Retenção e Descarte de Informações

As informações são armazenadas em ambientes autorizados e gerenciados, preservando sua integridade e disponibilidade. A retenção de dados segue requisitos legais, contratuais e operacionais, evitando acúmulo desnecessário de informações. O descarte é realizado por meios

seguros, impedindo sua recuperação por terceiros. Informações impressas ou anotadas são destruídas de forma adequada quando não forem mais necessárias.

7.10 Compartilhamento de Informações e Relacionamento com Terceiros

O compartilhamento de informações com clientes, parceiros ou fornecedores ocorre de maneira controlada, restrita à necessidade e sempre alinhada com acordos de confidencialidade. Terceiros que tratam informações da Fitovision seguem requisitos contratuais compatíveis com os níveis de segurança definidos pela organização. A transferência de dados sensíveis considera meios seguros de transmissão e proteção durante todo o processo.

7.11 Monitoramento e Registro de Atividades

As atividades relevantes dos sistemas e serviços são registradas e monitoradas em níveis proporcionais à criticidade dos ambientes. Os registros permitem rastreabilidade, suporte à investigação de incidentes e análise de comportamento anômalo. O monitoramento é realizado de forma responsável e em conformidade com requisitos legais.

7.12 Gestão de Incidentes de Segurança

Eventos e incidentes de segurança são tratados de forma coordenada, seguindo processos formais de registro, análise e resposta. São mantidos mecanismos de monitoramento capazes de identificar ocorrências relevantes e apoiar o tratamento tempestivo. Investigações incluem análise da causa, impacto e ações necessárias para evitar recorrências. Evidências são preservadas e registradas de maneira adequada.

7.13 Continuidade Operacional e Recuperação

As operações críticas da Fitovision contam com práticas de continuidade e recuperação voltadas à manutenção da disponibilidade e à retomada segura dos serviços em cenários de interrupção. São realizados backups periódicos, com validações regulares de restauração, visando garantir a integridade e recuperação adequada das informações. Os procedimentos de contingência contemplam atividades essenciais e incluem monitoramento, resposta a incidentes, manutenções programadas, aplicação de medidas corretivas e ações de recuperação operacional. Em casos de indisponibilidade, a equipe técnica atua de forma controlada para diagnóstico, contenção e restabelecimento dos serviços no menor tempo possível, podendo ocorrer intervenções emergenciais para preservação da segurança, estabilidade e integridade dos ambientes.

7.14 Conformidade Legal, Regulatória e Normativa

A Fitovision garante conformidade com leis aplicáveis, incluindo a LGPD, bem como requisitos contratuais e normativos relacionados ao tratamento da informação. Processos e atividades críticas são avaliados regularmente quanto ao atendimento dessas obrigações. Não conformidades identificadas são tratadas de forma estruturada, promovendo melhoria contínua e redução de riscos.

8. Treinamento e conscientização

A Fitovision manterá programas obrigatórios de treinamento e conscientização em segurança da informação para todos os colaboradores, terceiros e prestadores envolvidos em atividades que tratem dados corporativos. O treinamento será aplicado no processo de integração (onboarding) e periodicamente, reforçando boas práticas, controles internos, políticas corporativas e responsabilidades individuais.

9. Conformidade e Consequências

O cumprimento desta Política de Segurança da Informação é obrigatório e constitui parte integrante das responsabilidades associadas às atividades exercidas na Fitovision. Qualquer violação às diretrizes aqui estabelecidas será analisada conforme a gravidade do fato, considerando circunstâncias, impactos e reincidência. A organização mantém um processo disciplinar que poderá ser aplicado em situações de descumprimento, incluindo advertências, restrições de acesso, medidas corretivas e demais providências compatíveis com a legislação vigente e políticas internas. O objetivo desse processo é preservar a segurança das informações, manter a conformidade institucional e assegurar um ambiente profissional íntegro e confiável. Esta política será revisada periodicamente para refletir mudanças tecnológicas, legais e operacionais.

Histórico de Versões

Versão: 1.0	Publicação Inicial