SOLO FORTE
AGROPECUÁRIA

2025 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

SOLO FORTE AGROPECUÁRIA	**Política de Segurança Da Informação** Classificação: Interna	**PSI-001-2025** **Versão:1.1** Última Revisão:24/11/2025

1. Introdução

A Solo Forte é uma empresa de agronegócio independente e sem quaisquer vínculos comerciais e/ou administrativos com outras organizações. Tem por finalidade contribuir para a qualidade da produção agropecuária nas principais regiões de Minas Gerais através das vendas e prestação dos seguintes produtos e/ou serviços: fertilizantes, ração e consultorias personalizadas de acordo com as necessidades do cliente.

A Solo Forte se preocupa com a integridade de seus funcionários e clientes, procurando utilizar a tecnologia e a internet para promover e impor limites que estabeleçam o bem-estar dos mesmos. Contudo, com o avanço continuamente acelerado da tecnologia se torna cada vez mais difícil promover um ambiente totalmente seguro e livre de incidentes que possam representar riscos aos princípios da empresa. Portanto, se faz necessária a implementação de meios vigorosos para mitigar as situações citadas.

Assim sendo, o presente documento visa auxiliar na elaboração de uma Política de Segurança da Informação, em conformidade com a Lei Geral De Proteção de Dados(LGPD), no que tange os tópicos de confidencialidade, integridade e disponibilidade institucional dos dados reservados - ISO/IEC 27001:2022. Os quesitos de reputação e confiabilidade institucionais se fazem portanto pertinentes e resguardam os fundamentos dos procedimentos empresariais. Em prol da confiabilidade informacional da empresa, é importante salientar a necessidade da compreensão e o cumprimento das mesmas por parte dos funcionários.

Ressalta-se que para os resultados da proteção de ativos serem alcançados com sucesso, se faz obrigatória a obediência às políticas documentadas, independentemente do nível hierárquico. Isto é, as políticas deste documento se aplicam a todas as pessoas físicas contratadas.

2. Propósito

Este documento possui como propósito estabelecer as diretrizes e normativas a serem seguidas pela organização Solo Forte com a finalidade de promover um ambiente seguro em relação aos princípios da companhia. As políticas implementadas visam proteger os ativos informacionais tangentes aos respectivos escopos da companhia, de seus funcionários e clientes, de forma a garantir a continuidade dos processos e a saúde institucional. À maneira institucional, os tópicos referenciados como confidencialidade, integridade e disponibilidade são cruciais como os três pilares no que envolve o campo de Segurança da Informação, conforme mencionado anteriormente:

- **Confidencialidade**: Deve-se restringir o acesso informacional ao funcionário em conformidade com o polo e setor de atuação. Funcionários de setores diferentes não devem possuir acesso ao mesmo tipo de dado. As informações de consumidores devem manter-se restritas no âmbito da empresa e um consumidor não deve conseguir visualizar informações internas de outro.
- **Integridade**: O processamento dos dados contidos necessita ser completamente conciso e compatível com o que foi apresentado anteriormente. Apenas especialistas ou funcionários específicos para determinada atividade devem gerenciar o processamento de dados da mesma.

- **Disponibilidade**: As informações devem estar acessíveis ao escopo autorizado durante o tempo todo. Quando um usuário com autorização necessitar operar os respectivos dados não deve se deparar com erros de queda ou inviabilidade na utilização do serviço.

Por conclusão, a organização se baseia na fundamentação de cada uma das três configurações mencionadas como parâmetros aos aspectos de controles adequados, como a estrutura organizacional, funções de software e hardware, e procedimentos; a fim de canalizar as regras de implementação de um SGSI quanto ao contexto das demandas da Solo Forte e seu modo de funcionamento.

3. Gerenciamento de Acesso

3.1. Controle de Acesso Lógico

3.1.1 Cada funcionário recebe credenciais de endereço email com iniciais padronizadas no formato "YY.nome@hotmail.com" por departamento e uma senha para acessar a rede LAN particular de seu setor. As seguintes iniciais são utilizadas para representar email cada departamento:

- Departamento Administrativo-Financeiro: "FI".
- Departamento Comercial e de Campo: "CC".
- Departamento de Operações e Logística: "OL".
- Departamento Técnico e de Inovação: "TI".
- Diretoria Executiva:"D*".

Em obediência ao modo administrativo institucional, ao Departamento Técnico e de Inovação atribui-se característica única e exclusiva de acesso direto ao modem para a troca do identificador e/ou senha global(is).

3.1.2 Apenas os membros pertencentes à diretoria executiva possuem perfis com configurações predefinidas para automaticamente utilizar a autenticação de dois fatores através de credenciais fornecidas. Os funcionários das filiais não possuem essa opção.

3.1.3 O banco de dados da organização registra ativamente a hora e os detalhes dos processos executados por cada usuário no sistema. Os registros ocorrem listados em uma lista vertical na seguinte ordem de prioridade:

1. Matriz Laboratorial: No topo da lista encontram-se os usuários que trabalham na unidade central da organização.
2. Filial Industrial: Profissionais pertencentes ao ramo da fabricação dos produtos se encontram em segundo lugar de prioridade na lista.
3. Filial Logística: Os profissionais da unidade responsável pelo despacho das encomendas se encontram em terceiro lugar de prioridade na lista.
4. Filial de Armazenamento: A unidade responsável por armazenar os produtos se encontra em quarto lugar de prioridade na lista.

3.1.4 Os arquivos de cláusulas contratuais são protegidos por uma criptografia em algoritmo SHA-256. Estes dados expiram diariamente e constam continuamente atualizados na caixa de entrada dos endereços de email com identificação referente ao Departamento Comercial e de Campo.

3.1.5 As respectivas sessões de login em quaisquer plataformas de terceiros e afins para a realização das atividades corporativas expiram a cada doze horas, dentro do período legal de efetivação das atividades organizacionais.

3.2. Controle de Acesso Físico

3.2.1. Durante o horário comercial, no que se relaciona ao trânsito no ambiente organizacional, será requisitada a apresentação do crachá identificador para procedimentos de saída e entrada presencial. As

catracas nas entradas das edificações serão os instrumentos de entrada e saída para com o uso do crachá.

3.2.2. O livre acesso a quaisquer salas ou ambientes de alto nível da empresa deve exigir a biometria facial por parte do usuário.

3.2.3. O acesso aos servidores físicos de cada unidade é protegido por uma fechadura eletrônica cuja senha é conhecida apenas pela equipe do Departamento Técnico e de Inovação. Essa senha não deve ser compartilhada.

3.2.4. Cada unidade engloba um sistema de videomonitoramento ativo por vinte e quatro horas diárias, no que se refere às políticas de retenção de imagens nos espaços públicos da empresa.

3.2.5. Pessoas não diretamente relacionadas ao contexto de exclusividade corporativa, como consumidores ou visitantes, obrigatoriamente serão acompanhadas de um profissional qualificado pelos seguintes requisitos:

- Minimamente um ano de permanência contratual na companhia.
- Pertencimento ao setor do Departamento Administrativo-Financeiro.
- Autorização prévia por parte do gerente do departamento para realizar o acompanhamento.
- Disponibilidade ininterrupta para o acompanhamento integral durante o tempo previsto.

Cabe ao escopo dos gerentes determinar situações ou eventualidades específicas em que não caberá demandar o acompanhamento do público-alvo.

3.2.6. Os consumidores contratantes de serviços terão uma cópia documentada das cláusulas constatadas no ato de assinatura do contrato. O documento original permanecerá sob posse do setor referente ao Departamento de Comércio e Campo da região contactada pelo cliente.

3.2.7. Se faz terminantemente proibido o compartilhamento de quaisquer instrumentos com fins corporativos para a execução de atividades enquanto no âmbito empresarial. Esta categoria abrange os seguintes dispositivos:

- Computadores e notebooks ou componentes de hardware.
- Dispositivos IoT.
- Conectores e Mouses.
- Adaptadores USB ou Wireless.
- Teclados e Mouses.

4. Plano de Contingência

4.1. Objetivo

Institui-se como fundamental o planejamento para lidar com situações emergenciais em que os serviços considerados essenciais, de acordo com a declaração de cada setor, sejam temporariamente afetados por uma dada condição. Como tal, realiza-se a implementação individual de protocolos de segurança a serem seguidos por cada departamento da Solo Forte em acordo com as necessidades específicas dos setores de atuação, sendo de suma importância enfatizar que o Departamento Técnico e de Inovação não assume controle autoritário para considerar o que é essencial no escopo de cada setor, mas sim apenas do seu próprio. Visando adequar o planejamento de medidas aos padrões recomendados, a companhia segue o sistema de análise e prevenção de riscos especificados conforme SGQ da normativa ISO 9001:2015.

4.2. Incêndios

Há cenários em que os servidores podem apresentar defeitos ou uma sobrecarga elevada de dados. Esse superaquecimento, embora mais comum em servidores propriamente ditos, também pode ocorrer relacionado a qualquer categoria de computadores e colocar em risco a integridade física tanto humana quanto institucional da companhia.

Para isso, nas localidades em que tem-se computadores e dispositivos relativamente comuns do ponto de vista da corporação, tem-se instalações contendo aparelhos detectores de fumaça. Os profissionais devem estar devidamente treinados para utilizar os extintores de incêndio mais próximos e lidar corretamente com a situação - ABNT NBR 12693:2021, CB-024. Já em razão da observância dos servidores como os núcleos de sustento do tráfego informacional, se faz imprescindível a constituição material rígida com garantia à proteção contra fogo. Com a finalidade de seguir essa condição, se constitui em cada unidade uma sala-cofre com revestimento corta-fogo e piso previamente testados para suportar condições extremas de temperatura - ABNT NBR 15247:2004, CB-024.

Ao passo que as implementações são feitas, se garante que os dados sensíveis como o sustento para a operabilidade integral da empresa, não sejam comprometidos ou permanentemente perdidos por acúmulo de calor ou umidade no ambiente.

4.3. Falta de Energia

A queda de energia é um cenário recorrente em situações de adversidades climáticas muito bruscas e é um potencial a ser considerado quanto à saúde dos equipamentos nos confins institucionais. Principalmente quando se levando em conta oscilações contínuas no fornecimento de energia, como em picos marcados por queda e retorno repentinos nos circuitos elétricos, a falha na integridade das informações e continuidade dos processos institucionais é representada como o principal fator de risco.

Levando isso em conta, a instituição preza pela utilização de aparelhos nobreak em todos os ramos categóricos de dispositivos computadores para a disponibilização constante de energia, prevenindo também situações que representem riscos graves quanto ao funcionamento ou expectativa de vida tecnológica informacional a longo prazo, como sobrecarga elétrica ou curto circuito. O perfil normativo de operabilidade utilizado por todos e quaisquer meios tecnológicos empregados nos limites da empresa se baseia em um nobreak do tipo on-line , com o propósito de evitar demoras para o tempo de resposta informacional em casos extremos - ABNT NBR 15014:2003, CB-03.

4.4. Descargas Atmosféricas

Dentro dos perímetros possíveis e visando evitar a ocorrência de descargas elétricas e proteger a segurança de suas informações tecnológicas, seus bens e funcionários, a Solo Forte emprega o uso vigente do Sistema de Proteção Contra Descargas Atmosféricas(SPDA) do tipo esfera rolante em suas edificações, comumente referenciado como o equipamento para-raios - ABNT NBR 5419:2015, CB-03. O método implanta captores nas regiões do edifício com maior probabilidade de incidência, sendo a condição ideal para a Solo Forte. Ressalta-se que efeitos de magnitude indiretamente causados, tanto nos escopos humanos quanto tecnológicos, não se declaram como totalmente descartáveis embora minimizados: paradas cardíacas ou fenômenos de interferência eletromagnética por exemplo não podem ser garantidamente impedidos.

Ao passo que as regras de uso preestabelecidas pela SPDA estabelecem diferentes níveis de proteção conforme o material e propósito arquitetônico da estrutura, determina-se a utilização do Nível de proteção II para as filiais como detentoras de foco computacional robusto. A matriz como um centro laboratorial englobado por produtos químicos, emprega o uso do Nível de Proteção I.

5. Segurança de Redes e Comunicações

5.1. Proteção de redes

5.1.1 Regras de Firewall

Em acordo vigente com a proteção contra violações de segurança e privacidade na comunicação, a instituição determina o uso de roteadores com firewall dedicado nas filiais e na matriz, seguindo as instruções da seção de Zonas de Rede, 7.2.3 da ISO/IEC 27033-2:2012. Dito isso, as políticas locais de segurança ditadas ao modem bloqueiam o acesso à rede particular para quaisquer tentativas de acesso externas à rede corporativa por identificação de origem do IP do dispositivo. Apenas máquinas identificadas pela rede local dos departamentos são autorizadas. Os visitantes e clientes possuem poder de acesso apenas às redes públicas disponibilizadas pelos departamentos, que autorizam o acesso à qualquer dispositivo independentemente do IP de origem detectado.

Nesses termos, o filtro de pacotes de rede permitirá ou negará o acesso à rede wireless a dispositivos através da checagem das informações de IP de origem/destino e o protocolo de conexão requerido pelo pacote de dados recebido.

Como necessidade quanto à constituição e adoção de padrões conhecidos para adicionar camadas de segurança entre a rede interna confiável e a internet, a organização utiliza uma zona DMZ na rede wireless comercial e hospeda seus serviços dentro desse perímetro, conforme ISO/IEC 27033-2:2012. Com essa implementação, serviços como a página web e o DNS são isolados em um ambiente diferente da LAN, permitindo aos consumidores que verifiquem objetivamente apenas as informações do serviço, mas não da rede de origem. Essa prática busca limitar o acesso externo a qualquer tipo de informação da rede interna local da empresa por parte da internet.

5.1.2 Proteção Contra Spams Via Email

Para amenizar situações de ataques por anexos de links contendo arquivos maliciosos ou corrompidos enviados e/ou recebidos via endereços de email, o DNS interno da empresa está configurado para identificar padrões de domínios remetentes de mensagens caracterizadas como phishing e gradualmente bloqueá-los das vias de comunicação de sua rede particular. Assim, a instituição impede, a nível de rede, o acesso aos sites identificados nos filtros de DNS e redireciona o usuário para uma página de erro, impedindo o acesso ao domínio contendo malware. Para isso, a empresa segue as definições de proteção contra vazamento de dados e promove conscientização de seus colaboradores, conforme consta na normativa ISO/IEC 27001:2022.

Além disso, conforme configuração de usurpação de identidade, seja por meio de uma pessoa física ou jurídica, os protocolos de DNS auxiliam na prevenção contra técnicas em que usuários não autenticados tentem enviar e-mails em nome da organização. Com isso em mente, os departamentos têm seus registros configurados explicitamente para determinar os servidores de email autorizados.

5.2. Monitoramento e detecção de intrusão

5.2.1 Análise de dados

Ao modo que o monitoramento cumulativo do tráfego se faz necessário no que se refere à privacidade dos dados corporativos, a Solo Forte faz o uso legal de ferramentas de software para capturar e interceptar os dados presentes em sua rede particular. Cada departamento abriga uma máquina com o software Wireshark para análise dos pacotes recebidos pela comunicação com as redes públicas e particulares disponibilizadas, conforme referenciado na normativa ISO/IEC 27033-2:2012 como teste de segurança utilizando “network sniffing”.

A equipe do Departamento Técnico e de Inovação se responsabiliza pelo monitoramento das máquinas com o Wireshark instalado e a análise granular da captura do protocolo e do conteúdo das conexões direcionadas para dentro e fora da rede.

5.2.2 Metrificação de dados

A instituição configura como necessária a obtenção de parâmetros explícitos para quantificar a performance da rede e dos dispositivos conectados como forma de identificação de falhas ou inconsistências que possam vir a acarretar em problemas sérios. Leva-se em conta as definições de design apontadas na normativa ISO/IEC 27033-2:2012 e a indicação específica feita na seção 8.4 sobre a inclusão de monitoramento para identificação de problemas antes que possam afetar ao usuário. Portanto, a empresa emprega o uso de uma máquina contendo a solução de software Zabbix em cada departamento como meio de metrificação dos estados dos equipamentos e a emissão de alertas para quando as condições de erro são satisfeitas.

A equipe do Departamento Técnico e de Inovação se responsabiliza pelo monitoramento das máquinas com Zabbix instalado e assegura o ajuste da rede conforme identificação de vulnerabilidades, sistemáticas ou não, que possam impactar negativamente em seu fluxo de funcionamento ou seus componentes.

6. Gestão Ambiental

6.1. Objetivo

A constituição da Solo Forte identifica a necessidade da priorização de medidas proativas para o desenvolvimento sustentável e aplicação holística de métodos para a amenização dos riscos ambientais originados pelas atividades da organização, envolvendo todos os aspectos possíveis de impacto ambiental. Isto posto, a Diretoria Executiva entende como dever o exercício para a elaboração de um SGA como guia organizacional - ISO 14001:2015, com base na metodologia Plan-Do-Check-Act. A Solo Forte compreende a importância do desenvolvimento sustentável principalmente tratando-se de seu ramo de atuação: o agronegócio.

6.2. Medidas de Segurança

A Diretoria Executa lista uma série de medidas para estabelecer políticas ambientais, identificar aspectos e impactos ambientais, e monitorar a performance ambiental de todas as unidades da Solo Forte, incluindo o centro laboratorial. As medidas se caracterizam pelos seguintes fatores:

- **Controle de Uso dos Agrotóxicos**: A matéria-prima para a produção dos insumos da empresa pela Filial de Fabricação é continuamente monitorada com o uso mínimo de agrotóxicos e que não sejam de risco inaceitável.
- **Análise Laboratorial de Insumos:** A matriz ou centro laboratorial da Solo Forte realiza testes químicos nos insumos produzidos e descarta-os em lixo tóxico caso apresentem indícios condicionais impróprios para adubo.
- **Prática de Rotação de Culturas:** A organização aplica continuamente as práticas de rotação de culturas a fim de amenizar a exaustão do solo e promover sua conservação.
- **Análise Pós-Plantio:** Após a colheita de uma safra, a Filial de Fabricação se responsabiliza por analisar as condições de pH solo e executar medidas para correção química conforme necessário.
- **Controle dos Componentes Presentes na Ração:** Caso algum animal apresente reações à ração entregue, o Departamento Comercial e de Campo se responsabiliza por atender ao cliente para analisar o caso e substituir a ração se necessário.

7. Conscientização e Treinamento em Segurança

7.1 Programa de conscientização

7.1.1 Objetivos e Estrutura

A Solo Forte compreende que a tecnologia, por si só, não garante a segurança total se o fator humano não estiver alinhado às políticas de proteção. Portanto, institui-se um programa de conscientização obrigatório para todos os colaboradores (efetivos e terceirizados), visando mitigar riscos associados à Engenharia Social e ao uso indevido dos ativos corporativos. O programa será gerido pela equipe de segurança da informação e integrará as seguintes etapas:

- **Integração (Onboarding):** Apresentação das normas de segurança no ato da contratação, com ênfase nas responsabilidades descritas na seção de Responsabilidades.
- **Comunicados Periódicos:** Envio mensal de Orientações para os endereços de email corporativos, respeitando a padronização definida no departamento (formato “YY.nome@hotmail.com”), reforçando alertas sobre novas ameaças no setor do agronegócio.

- **Simulação de Phishing:** Realização de testes práticos enviando e-mails falsos controlados para verificar a atenção dos colaboradores, complementando as proteções técnicas de DNS já implementadas na proteção contra spams.

7.1.2 Temáticas Obrigatórias

O conteúdo programático deve abordar situações cotidianas que impactam a confidencialidade e integridade da empresa, incluindo:

- **Segurança de Credenciais:** Orientação estrita sobre a não partilha de senhas de acesso lógico e códigos de fechaduras eletrônicas dos servidores, conforme estipulado nas políticas de controle de acesso.
- **Acesso Físico e Vigilância:** Reforço sobre a obrigatoriedade do uso de crachás e a proibição da entrada de visitantes desacompanhados em áreas restritas, respeitando as regras de acesso físico descritas anteriormente.
- **Uso de Dispositivos Pessoais**: Reiteração da proibição de conectar dispositivos particulares (como USBs e periféricos) na rede corporativa ou computadores da empresa, prevenindo a introdução de malwares conforme a política de proibição de compartilhamento.
- **Resposta a Incidentes**: Instrução clara sobre como e quando reportar anomalias ou suspeitas de violação à equipe responsável, garantindo a agilidade prevista no plano de contingência.

7.2. Treinamento em Segurança

7.2.1 Diretrizes para a Realização dos Treinamentos

A solo forte estabelece que todos os treinamentos de Segurança da Informação devem seguir diretrizes claras para garantir sua eficácia e aplicabilidade no ambiente agropecuário. Os treinamentos devem:

- Ser adaptados aos diferentes setores da empresa, considerando colaboradores do campo, do escritório, operadores de máquina, equipes técnicas e administrativos.
- Utilizar exemplos práticos do dia a dia da empresa, como o uso seguro de tablets em campo, proteção de dados coletados por sensores e drones, e cuidados na transmissão de informações sobre os produtos comercializados e sobre os clientes.
- Serão realizados em formato presencial ou remoto, permitindo flexibilidades para equipes operacionais que trabalham em fazendas, galpões e áreas externas.
- Ser atualizados sempre que houver mudanças tecnológicas, implementação de novos sistemas agrícolas, adoção do IoT, máquinas inteligentes ou identificação de novas ameaças.

7.2.2 Frequência e Atualização dos Treinamentos

A Solo forte estabelece que os treinamentos de segurança sejam realizados de forma contínua, garantindo que todos os colaboradores mantenham um nível adequado de conhecimento e preparo para lidar com riscos atuais e emergentes. Como regra geral, os treinamentos devem ocorrer anualmente, cobrindo os princípios essenciais de segurança, boas práticas e as normas internas da empresa. Para equipes que lidam diretamente com dados sensíveis ou com tecnologias de campo, sensores, drones, sistemas de monitoramento e análise de solo serão realizados reciclagem semestrais, permitindo que esses profissionais estejam sempre atualizados quanto às melhores práticas de proteção de dados.

Além disso, sempre que ocorrerem mudanças significativas nos sistemas utilizados, na infraestrutura tecnológica ou no ambiente de ameaças, treinamentos extraordinários deverão ser realizados para garantir a adaptação imediata dos colaboradores. O conteúdo também deve ser periodicamente revisado e atualizado para refletir a evolução do cenário de risco no setor agropecuário, considerando novas técnicas de ataque, tentativas de fraude e particularidades das operações rurais. Todas as participações deverão ser registradas e monitoradas pela área responsável, servindo como evidência de conformidade e como base para auditorias internas e melhorias contínuas.

8. Avaliação e Melhoria Contínua

8.1. Auditorias de segurança

8.1.1. Planejamento e Execução

Visando assegurar a conformidade com os requisitos estabelecidos na ISO/IEC 27001:2022, a Solo Forte institui a obrigatoriedade de auditorias internas periódicas. A responsabilidade pela condução dessas auditorias recai sobre a Equipe de Segurança da informação, que deverá realizar verificações semestrais para validar e eficácia dos controles implementados. O objetivo primordial é confrontar as políticas documentadas com a prática operacional, garantindo que as ferramentas de monitoramento e os protocolos de acesso físico e lógico estejam sendo executados conforme o planejado, identificando desvios antes que se tornem incidentes críticos.

8.1.2. Procedimentos de Verificação

As auditorias devem seguir um roteiro técnico rigoroso que inclua, minimamente, a revisão dos seguintes ativos e processos já estabelecidos na organização:

- **Monitoramento de Rede**: Análise amostral dos logs gerados pelo software Wireshark e verificação do histórico de alertas de performance emitidos pelo Zabbix, assegurando que a equipe técnica está tratando as vulnerabilidades apontadas pelas ferramentas de detecção.
- **Controle de Acesso Lógico:** Checagem da base de dados de usuários para confirmar se as prioridades de acesso (Matriz, Filial industrial, Logística) estão sendo respeitadas e se contas de ex-funcionários foram devidamente revogadas.
- **Integridade Física:** Inspeção in loco dos dispositivos de segurança ambiental, validando a operabilidade dos sistemas de nobreak e a manutenção das salas-cofre e extintores, em conformidade com as normas ABNT NBR 15014:2013 e NBR 12693:2021 citadas nas políticas de prevenção.
- **Conformidade de Criptografia:** Verificação aleatória nos arquivos contratuais para garantir que a criptografia SHA-256 está sendo aplicada corretamente nos documentos do Departamento Comercial e de Campo.

8.2. Revisão de políticas e procedimentos

8.2.1 Responsabilidade pela Revisão e Atualização

A responsabilidade pela revisão e atualização das políticas e procedimentos de Segurança da Informação da Solo Forte é atribuída à área designada para a gestão de segurança, que deve atuar em conformidade com as diretrizes das normas ISO/IEC 27001:2022 (controle A.5.1) e ISO/IEC 27002:2022. Essa equipe deve monitorar continuamente mudanças tecnológicas adotadas nas operações agropecuárias, alterações no cenário de ameaças e requisitos legais ou regulatórios que possam impactar o ambiente de segurança da empresa.

Cabe a essa área conduzir análises estruturadas, reunir informações relevantes, consultar especialistas internos e externos quando necessário, e propor atualizações consistentes nos documentos. Todas as revisões devem ser formalmente registradas, mantendo histórico de versões conforme recomendado pela ISO/IEC 27002:2022, garantindo rastreabilidade e integridade do processo. Além disso, a área responsável deve assegurar que todos os colaboradores recebam comunicação tempestiva sobre quaisquer alterações realizadas, reforçando a conformidade, a transparência e a adoção das práticas atualizadas em todo o ambiente operacional da Solo Forte.

8.2.2 Critérios para Revisão das Políticas e Procedimentos

O processo de revisão das políticas e procedimentos de Segurança da Informação da Solo Forte deve seguir critérios alinhados às recomendações das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, de forma a assegurar consistência, atualização e aderência ao cenário de riscos da empresa. A revisão deve considerar as mudanças tecnológicas aplicadas às atividades agropecuárias, como novos sistemas de gestão rural, sensores IoT, drones, softwares de análise de solo e plataformas de monitoramento operacional.

Também devem ser avaliadas as ameaças cibernéticas emergentes, os resultados de auditorias internas e externas, as lições aprendidas com incidentes anteriores e quaisquer atualizações legais ou regulatórias relacionadas à proteção de dados e ao setor agropecuário. Recomenda-se ainda que as revisões considerem as demandas operacionais das equipes de campo e administrativas, garantindo que os controles de segurança reflitam a realidade prática da Solo Forte. Esses critérios permitem que a empresa mantenha políticas robustas, atualizadas e alinhadas às melhores práticas internacionais.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

9.1.1. Proteção de Dados e Privacidade (LGPD)

Reiterando o compromisso firmado na introdução deste documento, a Solo Forte adere integralmente as disposições da Lei Geral de Proteção de Dados(Lei nº 13.709/2018). Todas as atividades de coleta, processamento e armazenamento de informação de clientes e colaboradores devem respeitar os princípios de finalidade e necessidade. Isso se aplica especialmente ao manuseio dos dados contratuais criptografados (mencionados no item 3.1.4) e as informações dos consumidores, garantindo que o isolamento de dados entre diferentes clientes, previstos na política de confidencialidade, seja rigorosamente mantido para evitar vazamentos ou acessos cruzados indevidos

9.1.2. Legalidade do Monitoramento e Marco Civil

As práticas de vigilância tecnológica adotadas pela organização, incluindo o monitoramento de tráfego de rede via Wireshark e a captura de imagens pelo sistema de videomonitoramento 24h, são realizadas

em estrita conformidade com o Marco Civil da Internet (Lei nº 12.965/2014) e a legislação trabalhista vigente. Para garantir a transparência legal, a solo Forte assegura que:

- A coleta de logs de acesso e a interceptação de pacotes para análise de segurança são realizadas exclusivamente no ambiente corporativo e com ciência prévia dos colaboradores, visando apenas a proteção dos ativos e não a violação de intimidade.
- Os registros de acesso (logs) detalhados na seção de Gerenciamento de Acesso são mantidos de forma segura e inalterável pelo período legalmente exigindo, servindo como prova material em casos de incidentes ou disputas judiciais.

9.2. Gerenciamento de vulnerabilidades e patches

A Solo Forte estabelece um processo contínuo e estruturado para o gerenciamento de vulnerabilidades e aplicação de patches, com o objetivo de manter a integridade, disponibilidade e segurança dos sistemas utilizados nas operações agropecuárias. Esse processo segue as boas práticas definidas pelas normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, que recomendam a identificação, avaliação e tratamento sistemático de vulnerabilidades em tecnologias da informação.

O gerenciamento de vulnerabilidades compreende a identificação periódica de falhas em sistemas operacionais, softwares de gestão rural, dispositivos IoT instalados em campo, drones, sensores de solo, aplicações corporativas e demais recursos utilizados nas operações da Solo Forte. Ferramentas de varredura e análises técnicas devem ser empregadas para detectar pontos frágeis e avaliar seu nível de severidade. Com base nos riscos encontrados, a equipe responsável deve priorizar as correções, considerando a criticidade das operações agrícolas e os impactos potenciais de falhas ou indisponibilidades.

A aplicação de patches e atualizações de segurança deve ocorrer de forma controlada, planejada e documentada. Sempre que possível, atualizações devem ser testadas previamente em ambiente seguro, garantindo que não afetem o funcionamento de sistemas essenciais à produção, ao monitoramento do solo, ao gerenciamento de maquinário ou à coleta de dados em campo. Patches críticos, relacionados a vulnerabilidades com risco elevado, devem ser aplicados com prioridade, seguindo prazos compatíveis com o grau de ameaça identificado.

Além disso, todo o processo deve contemplar o monitoramento contínuo de fornecedores de softwares, fabricantes de sensores, plataformas de drones e sistemas agrícolas, assegurando que novas atualizações, alertas ou correções recomendadas sejam identificadas e aplicadas de forma tempestiva. O histórico de vulnerabilidades detectadas, patches aplicados e prazos de execução deve ser mantido para fins de auditoria, melhoria contínua e comprovação de conformidade com a política de segurança.

O gerenciamento eficaz de vulnerabilidades e patches fortalece a resiliência tecnológica da Solo Forte, reduz riscos operacionais, e garante a continuidade e a confiabilidade das atividades agrícolas e administrativas que dependem de recursos digitais.

9.2.1 Identificação e Avaliação de Vulnerabilidades

A Solo Forte estabelece um processo contínuo e estruturado para o gerenciamento de vulnerabilidades e aplicação de patches, com o objetivo de manter a integridade, disponibilidade e segurança dos sistemas utilizados nas operações agropecuárias. Esse processo segue as boas práticas definidas pelas normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, que recomendam a identificação, avaliação e tratamento sistemático de vulnerabilidades em tecnologias da informação.

O gerenciamento de vulnerabilidades compreende a identificação periódica de falhas em sistemas operacionais, softwares de gestão rural, dispositivos IoT instalados em campo, drones, sensores de solo, aplicações corporativas e demais recursos utilizados nas operações da Solo Forte. Ferramentas de varredura e análises técnicas devem ser empregadas para detectar pontos frágeis e avaliar seu nível de severidade. Com base nos riscos encontrados, a equipe responsável deve priorizar as correções, considerando a criticidade das operações agrícolas e os impactos potenciais de falhas ou indisponibilidades.

A aplicação de patches e atualizações de segurança deve ocorrer de forma controlada, planejada e documentada. Sempre que possível, atualizações devem ser testadas previamente em ambiente seguro, garantindo que não afetem o funcionamento de sistemas essenciais à produção, ao monitoramento do solo, ao gerenciamento de maquinário ou à coleta de dados em campo. Patches críticos, relacionados a vulnerabilidades com risco elevado, devem ser aplicados com prioridade, seguindo prazos compatíveis com o grau de ameaça identificado.

Além disso, todo o processo deve contemplar o monitoramento contínuo de fornecedores de softwares, fabricantes de sensores, plataformas de drones e sistemas agrícolas, assegurando que novas atualizações, alertas ou correções recomendadas sejam identificadas e aplicadas de forma tempestiva. O histórico de vulnerabilidades detectadas, patches aplicados e prazos de execução deve ser mantido para fins de auditoria, melhoria contínua e comprovação de conformidade com a política de segurança.

O gerenciamento eficaz de vulnerabilidades e patches fortalece a resiliência tecnológica da Solo Forte, reduz riscos operacionais, e garante a continuidade e a confiabilidade das atividades agrícolas e administrativas que dependem de recursos digitais.

10. Responsabilidades

10.1. Direção

10.1.1. Governança e Compromisso Estratégico

A Alta Direção da Solo Forte assume a responsabilidade final pela eficácia do Sistema de Gestão de Segurança da Informação (SGSI). Cabe aos membros da Diretoria Executiva (identificados pelo prefixo "D*" nos e-mails corporativos) estabelecer as diretrizes de segurança alinhadas aos objetivos de negócio do agronegócio, garantindo que a política de segurança não seja apenas um documento burocrático, mas uma prática ativa. Além de aprovar as políticas, a Direção deve liderar pelo exemplo, aderindo rigorosamente aos controles restritos, como a utilização obrigatória de autenticação de dois fatores (2FA) em seus acessos, conforme definido nas políticas de controle lógico.

10.1.2. Provisão de Recursos

É dever da direção assegurar que os recursos financeiros, tecnológicos e humanos necessários estejam disponíveis para a implementação e manutenção dos controles de segurança descritos neste documento. Isso inclui a aprovação de orçamento para:

- **Infraestrutura de Proteção:** Manutenção dos sistemas de alto custo, como a sala-cofre com revestimento corta-fogo e os sistemas de proteção contra descargas atmosféricas (SPDA) instalados nas filiais e matriz.
- **Ferramentas de Monitoramento:** Aquisição e renovação de licenças ou suporte para as soluções de software utilizadas na gestão de rede(Zabbix) e análise de tráfego.
- **Continuidade de Negócios:** Garantia de disponibilidade de equipamentos de contingência, como os nobreaks online, assegurando que a operação não pare diante de falhas elétricas.

10.2. Equipe de segurança da informação

10.2.1 Operação e Monitoramento Técnico

Subordinada ao Departamento Técnico e de Inovação, esta equipe detém a responsabilidade exclusiva pela execução operacional das ferramentas de defesa cibernética. Cabe aos seus integrantes a análise granular do tráfego de rede através do software **Wireshark** e o acompanhamento contínuo das métricas de desempenho e alertas de falhas emitidos pela solução **Zabbix**. Além disso, em conformidade com a gestão de acesso lógico, somente esta equipe possui autorização para realizar alterações críticas na infraestrutura de rede, como a troca dos identificadores e senhas globais dos modems da instituição

10.2.2. Gestão de Acessos Privilegiados e incidentes

A equipe atua como guardiã dos ativos mais sensíveis da Solo Forte, sendo a única detentora da senha das fechaduras eletrônicas que protegem os servidores físicos em cada unidade, sendo terminantemente proibido o compartilhamento desse segredo com outros setores. No âmbito da resposta a incidentes, é dever desta equipe receber, triar e investigar imediatamente as notificações de segurança reportadas pelos funcionários, iniciando os protocolos de contenção de danos e reparação de serviços conforme definido no Plano de Contingência.

10.3. Funcionários

Os funcionários da organização devem cumprir integralmente esta Política de Segurança da Informação, atuando sempre de forma responsável, ética e compatível com as normas internas e com os requisitos legais aplicáveis. Cada colaborador é responsável por proteger a confidencialidade, a integridade e a disponibilidade das informações às quais tem acesso, devendo tratar dados corporativos, pessoais, sensíveis ou estratégicos conforme os princípios estabelecidos pela ISO/IEC 27001 e controles da ISO/IEC 27002:2022. Toda informação utilizada no exercício das atividades deve ser manipulada com precisão, atualização e zelo, de modo a evitar erros, perdas ou exposição indevida.

Os funcionários devem utilizar sistemas, equipamentos, credenciais e demais recursos tecnológicos exclusivamente para finalidades autorizadas, sendo proibido qualquer uso que comprometa a segurança ou viole procedimentos internos. A proteção das credenciais é obrigatória, sendo vedado o compartilhamento de senhas ou meios de autenticação, devendo cada acesso ser utilizado apenas dentro do escopo das funções atribuídas. Informações devem ser classificadas e tratadas conforme sua sensibilidade, seguindo o procedimento de classificação e rotulagem definido pela organização e alinhado à ISO/IEC 27002:2022.

Todos os documentos, sejam físicos ou digitais, devem ser armazenados adequadamente e descartados de maneira segura, utilizando métodos de destruição apropriados, como fragmentação, trituração ou exclusão digital permanente certificada. A responsabilidade pela segurança estende-se ao uso de dispositivos móveis e acessos remotos, que devem seguir mecanismos de proteção estabelecidos, incluindo criptografia, senhas fortes, VPN e autenticação multifator sempre que aplicável.

Cada funcionário deve participar de treinamentos periódicos de conscientização em Segurança da Informação, mantendo-se informado sobre práticas seguras, riscos atuais e procedimentos de resposta. Qualquer incidente, suspeita de violação ou falha de segurança deve ser comunicado imediatamente ao responsável pelo SGSI, sendo a omissão considerada violação desta política. Ao término do vínculo ou alteração de função, o colaborador deve devolver todos os ativos corporativos, ter seus acessos revogados e manter permanentemente o dever de confidencialidade sobre todas as informações obtidas durante seu período de atuação.

11. Classificação da Informação

11.1. Pública

O nível informacional público denomina dados acessíveis tanto internamente, para agentes institucionais, quanto externamente, para clientes e/ou visitantes. Tem-se nessa modalidade as seguintes informações:

- Comunicados de funcionamento da empresa por notificações de e-mail.
- Comércio e venda dos produtos fornecidos.
- Vagas de emprego publicadas direta e exclusivamente pela instituição.

11.2. Interna

Constam-se informações disponibilizadas somente aos funcionários internos e independentemente do nível hierárquico representado pelos mesmos. Publicações de regras gerais referentes à ordem institucional encontram-se neste escopo. Os principais itens listados são:

- Manuais de sistemas internos.
- Atas de reuniões operacionais.
- Procedimentos com fins de adequação a situações de risco

11.3. Confidencial

Informações relevantes a nível de departamento ou setor distintos encontram-se no escopo “Confidencial”, em exceção da Diretoria Executiva, que detém documentação do escopo informacional de cada departamento além da própria. Em exigência à concretização sumária desse escopo, notificam-se os dados por cada departamento:

- **Departamento Administrativo-Financeiro:** Dados financeiros, contábeis e fiscais. Informações sobre folha de pagamento, benefícios, encargos e dados bancários. Acordos contratuais, negociações internas e documentos societários.
- **Departamento Comercial e de Campo:** Carteira de clientes e prospects. Estratégias comerciais, metas, indicadores e oportunidades de negócio com clientes. Dados sensíveis de clientes, contratos e históricos de atendimento.
- **Departamento de Operações e Logística:** Dados de estoque, suprimentos, transporte e rotas. Processos internos operacionais, fluxos de entrega e planejamento logístico. Informações sobre fornecedores, prazos e cadeia produtiva.
- **Departamento Técnico e de Inovação:** Documentação de sistemas, infraestrutura, APIs e integrações. Código-fonte, configurações internas, acessos administrativos e arquiteturas. Projetos de inovação, pesquisa interna e propriedade intelectual técnica.

Ressalta-se que a Diretoria Executiva detém poder sob todas as informações citadas e que cada departamento deve alinhar-se a qualquer atualização exigida.

11.4. Restrita

Conjuntos de dados extremamente sensíveis e unicamente visíveis ao departamento de Diretoria Executiva, responsável pelo nível estratégico da empresa. O principal conteúdo é sumarizado pelas seguintes regras:

- Revisão mensal de acessos.
- Acesso ao cofre da empresa.
- Monitoramento contínuo do tráfego monetário mensal, despesas e lucros.
- Acesso a informação da pessoa física de cada colaborador ativo.
- Gerenciamento de todas as licenças utilizadas.

12. APÊNDICE 2

2

2FA: Sigla para *Two-Factor Authentication* ou Autenticação de Dois Fatores, uma camada extra de segurança que exige duas formas distintas de identificação para liberar o acesso.

13. APÊNDICE A

A

ABNT: Nomenclatura para Associação Brasileira de Normas Técnicas, órgão responsável por ditar a normatização técnica no Brasil.

14. APÊNDICE C

C

CB-024: Nomenclatura de definição do Comitê Brasileiro de Segurança Contra Incêndio.

CB-03: Nomenclatura de definição do Comitê Brasileiro de Eletricidade.

CONFIDENCIALIDADE: Propriedade que denomina que apenas usuários autorizados podem acessar determinadas informações.

15. APÊNDICE D

D

DISPONIBILIDADE: Propriedade que denomina que as informações devem estar sempre acessíveis aos usuários autorizados.

DMZ: Denomina-se como Demilitarized Zone e se define como uma rede de perímetro que adiciona uma camada extra de segurança à rede interna contra o tráfego externo.

DNS: Denomina-se como Domain Name System e mapeia um nome de domínio humanamente legível para um endereço IP, permitindo o acesso na internet pelo nome de domínio escolhido.

16. APÊNDICE E

E

ENGENHARIA SOCIAL: Técnica de manipulação psicológica utilizada por criminosos para induzir usuários a realizarem ações indevidas ou divulgarem informações confidenciais.

17. APÊNDICE F

F

FIREWALL: Propriedade para determinar o controle da entrada e saída de tráfego em uma rede interna em relação à conexão global da internet, através de portas de conexão.

18. APÊNDICE H

H

HARDWARE: Nomenclatura técnica para componentes físicos constituintes de um computador.

19. APÊNDICE I

I

IEC: Nomenclatura para International Electrotechnical Commission, órgão responsável por ditar normativas globais específicas para tecnologias elétricas e eletrônicas.

INTEGRIDADE: Propriedade que denomina que as informações devem estar inteiras e sem modificações fora do padrão esperado.

ISO: Nomenclatura para International Organization For Standardization, órgão responsável por ditar a normatização técnica internacional.

ISO 9001:2015: Normativa estabelecida para seguir requisitos na implementação de um Sistema de Gestão de Qualidade, que foca na melhoria contínua dos processos através da conformidade operacional alinhada às exigências internas e externas da gestão de processos informacionais.

ISO 14001:2015: Normativa estabelecida para seguir requisitos na implementação de um Sistema de Gestão Ambiental, que enfatiza especificamente a regulamentação de regras para a preservação do meio ambiente e controle de ações que possam afetá-lo.

ISO/IEC 27001:2022: Normativa estabelecida pela International Organization for Standardization conjunta à International Electrotechnical Commission que define os principais requisitos necessários e exigidos para se implementar um Sistema de Gerenciamento da Segurança da Informação.

ISO/IEC 27002:2022: Normativa estabelecida pela International Organization for Standardization conjunta à International Electrotechnical Commission que especifica o guia sobre como melhorar e seguir boas práticas a fim de aperfeiçoar o funcionamento de um Sistema de Gerenciamento da Segurança da Informação

ISO/IEC 27033-2:2012: Normativa estabelecida pela International Organization for Standardization conjunta à International Electrotechnical Commission que especifica o guia de planejamento, design e implantação de uma rede segura.

20. APÊNDICE L

L

LAN: Nomenclatura para Local Area Network ou Rede Local, e conceitua o princípio de uma rede interna que conecta um grupo de computadores em uma área geográfica delimitada.

LGPD: Sigla para Lei Geral de Proteção de Dados (Lei nº 13.709/2018), legislação brasileira que regula as atividades de tratamento de dados pessoais.

21. APÊNDICE M

M

MALWARE: Nome técnico para software intencionalmente programado para prejudicar e causar interrupção ou vazamento de dados de dispositivos tecnológicos.

MARCO CIVIL DA INTERNET: Denominação da Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

22. APÊNDICE N

N

NBR 5419:2015: Normativa estabelecida pela Associação Brasileira de Normas Técnicas no Comitê Brasileiro de Eletricidade para estabelecer as condições do Sistema de Proteção Contra Descargas Atmosféricas contra incidência de raios.

NBR 12693:2021: Normativa estabelecida pela Associação Brasileira de Normas Técnicas no Comitê Brasileiro de Segurança Contra Incêndio como os termos de instalação de extintores de incêndio em edificações e áreas de risco.

NBR 15014:2003: Norma estabelecida pela Associação Brasileira de Normas Técnicas no Comitê Brasileiro de Eletricidade para a descrição das definições para sistemas de alimentação ininterruptas(nobreaks).

NBR 15247:2004: Normativa estabelecida pela Associação Brasileira de Normas Técnicas no Comitê Brasileiro de Segurança Contra Incêndio para a definição de testes e requisitos oriundos de uma sala-cofre.

NOBREAK: Nomenclatura que denomina um aparelho com sistema de alimentação de potência ininterrupta.

23. APÊNDICE P

P

PACOTE: Pequeno segmento de rede que possui informações dos dados recebidos pelo tráfego em uma rede.

PHISHING: Nomenclatura para caracterizar tentativas de ataque tecnológicas por meio de mensagens de email com anexos de arquivo ou conteúdo para roubo de dados.

PLAN-DO-CHECK-ACT: Denominação para um passo a passo constituído de quatro processos empresariais para a melhoria contínua dos processos, baseado na seguinte ordem:

1. **Plan**: Estabelecer objetivos e processos necessários para apresentar os melhores resultados.
2. **Do**: Executar os objetivos do passo anterior.
3. **Check**: Validar a execução do processo anterior.
4. **Act**: Modificar os processos removendo os erros apontados nos passos de execução e validação.

PORTA DE CONEXÃO: Interface numérica de um sistema ou dispositivo que identifica o ponto de entrada para conexão a um serviço e/ou aplicação específicos(as).

24. APÊNDICE R

R

ROTAÇÃO DE CULTURAS: A rotação de culturas é uma técnica agrícola de conservação que consiste em trocar os tipos de vegetal que são cultivados a cada ciclo de cultivo, como maneira para amenizar a exaustão contínua do solo por espécies vegetais que tenham necessidade de adubação muito elevadas.

25. APÊNDICE S

S

SGA: Nomenclatura para Sistema de Gestão Ambiental, que se refere à integração de políticas, procedimentos e processos específicos para melhorar a performance informacional organizacional em relação à preservação do meio ambiente.

SGSI: Denominação para Sistema de Gestão de Segurança da Informação, um conjunto de políticas e regras que uma organização usa para a proteção de seus dados, em conformidade com a lei e normas técnicas.

SGQ: Nomenclatura para Sistema de Gestão de Qualidade, que se refere a uma estrutura formal composta por critérios operacionais para denominar as principais regras de gestão dos processos corporativos.

SHA-256: Um algoritmo de criptografia que transforma texto humanamente legível em uma sequência encadeada de 256 bits totais de caracteres.

SOFTWARE: Nomenclatura técnica para programas de computador.

SPDA: Sigla para Sistema de Proteção contra Descargas Atmosféricas, conjunto de dispositivos (como para-raios) destinado a proteger estruturas contra os efeitos dos raios.

26. APÊNDICE W

W

WIRESHARK: Software open-source analisador de pacotes de rede de entrada e saída e seus protocolos, que demonstra informações dos dados transmitidos.

27. APÊNDICE Z

Z

ZABBIX: Solução de software para gerenciamento da saúde de ambientes de rede por meio da metrificação e visualização gráfica dos dados obtidos