POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SOLIDARIEDADE DIGITAL

> **“Protegendo Nossos Dados, Fortalecendo Nossa Missão”**
> *Uma política de segurança é um conjunto de diretrizes e práticas que visa proteger e gerenciar os recursos de uma organização, incluindo informações, ativos e tecnologias, e garantir a integridade, confidencialidade e disponibilidade desses recursos*

Bem-vindo(a) à sua Cartilha de Segurança Digital da ONG Solidariedade! Este guia foi feito para todos que usam, desenvolvem ou administram o sistema 'ONG Solidariedade' (um sistema em PHP com MySQL).

Nosso grande objetivo é claro: proteger os dados importantes das pessoas que atendemos, de nossos voluntários e parceiros. Queremos evitar que informações caiam em mãos erradas, sejam alteradas sem permissão ou que o sistema pare de funcionar.

Mesmo sendo um sistema CRUD (Cria, Lê, Atualiza, Deleta) em PHP e MySQL, e usando o XAMPP em desenvolvimento, a segurança é fundamental! Proteger nossos dados é proteger a confiança em nosso trabalho e a reputação da ONG

Esta política se aplica a desenvolvedores, administradores, colaboradores e parceiros que utilizam, mantêm ou têm acesso ao sistema e à infraestrutura relacionada, incluindo servidores locais e em nuvem (ex: AWS).

INTRODUÇÃO

Objetivo

Esta Política de Segurança da Informação (PSI) tem como principal objetivo estabelecer as diretrizes e práticas fundamentais para garantir a proteção e a confidencialidade das informações em todos os processos da "ONG Solidariedade", com foco especial no sistema "ONG Solidariedade" – uma aplicação CRUD (Create, Read, Update, Delete) desenvolvida em PHP com MySQL.

Nosso propósito é salvaguardar, de forma rigorosa, os dados sensíveis de todas as pessoas atendidas, voluntários e parceiros da ONG. Isso inclui protegê-los contra acessos não autorizados, vazamentos, alterações indevidas, perdas e falhas operacionais que possam comprometer a confiança, a reputação e a própria missão da nossa organização. Além disso, buscamos promover uma cultura de segurança da informação em toda a equipe, colaboradores e parceiros da ONG Solidariedade.

Escopo

Esta política abrange todos os membros da equipe da ONG Solidariedade (incluindo funcionários e voluntários), desenvolvedores, administradores e parceiros que utilizam, mantêm ou têm acesso ao sistema "ONG Solidariedade". O escopo inclui a infraestrutura tecnológica relacionada, abrangendo servidores locais, servidores em nuvem (como AWS) e quaisquer dispositivos (computadores, notebooks, celulares) utilizados para acessar esses recursos.

Importante: Esta política se aplica a todos os dados processados pelo sistema, independentemente do formato (digital ou físico) ou local de armazenamento, com atenção especial aos dados pessoais e sensíveis, conforme a legislação vigente.

PRINCÍPIOS ESSENCIAIS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação na ONG Solidariedade é baseada em quatro pilares fundamentais:

CONFIDENCIALIDADE

As informações e dados sensíveis devem ser acessíveis apenas por pessoas estritamente autorizadas e em conformidade com a necessidade de conhecimento para suas funções. A proteção da confidencialidade é assegurada por meio de rigorosos controles de acesso, autenticação forte e criptografia aplicada tanto a dados em trânsito quanto a dados armazenados, quando aplicável.

INTEGRIDADE

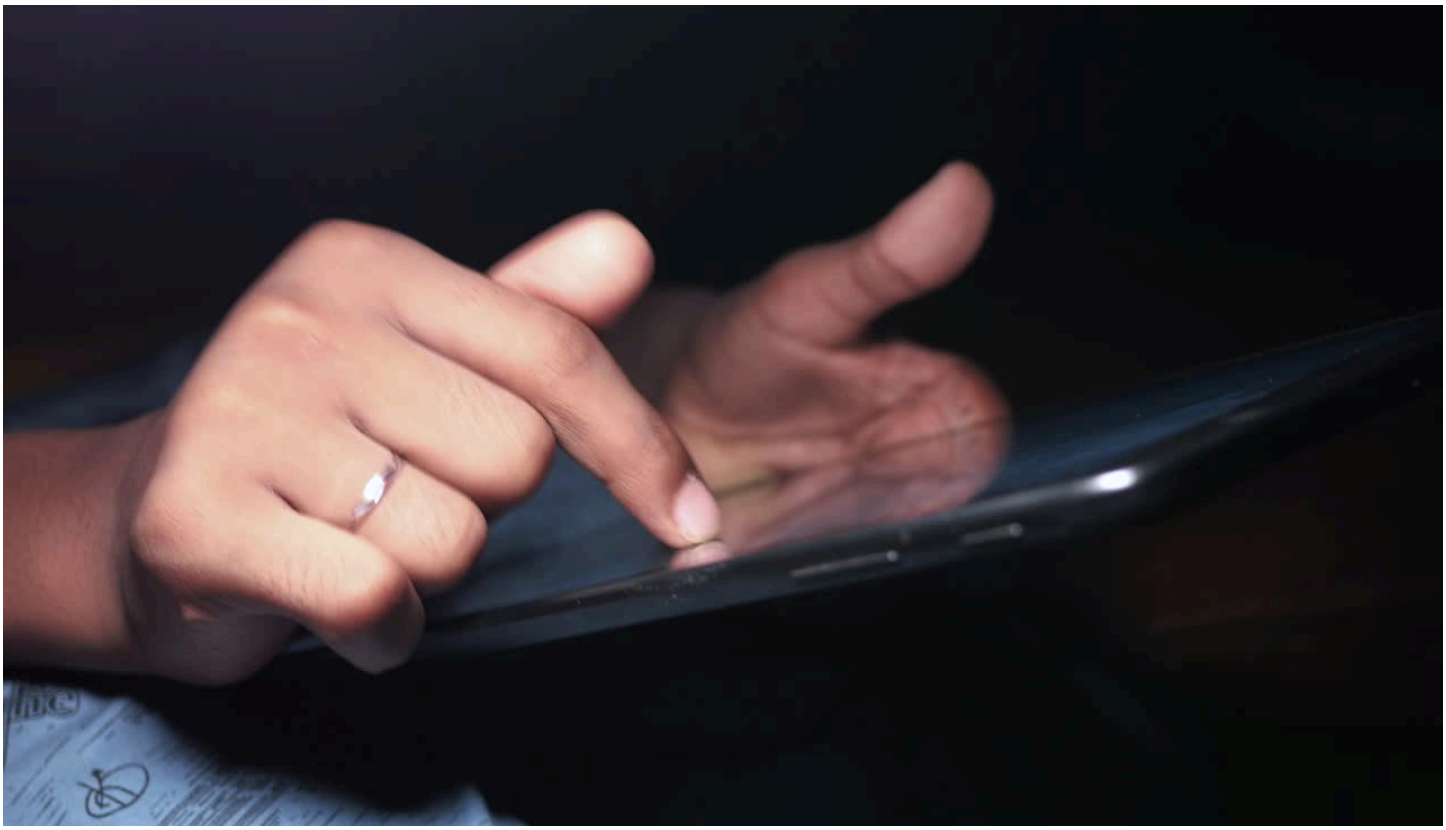
Os dados devem ser mantidos completos, precisos, consistentes e protegidos contra qualquer alteração não autorizada ou acidental. Isso inclui o uso de *prepared statements* (para evitar SQL Injection), sanitização e validação de entradas de dados, controle de permissões de acesso, além de mecanismos de validação e verificação de dados para garantir sua exatidão ao longo do tempo

DISPONIBILIDADE

O sistema e todos os dados devem estar acessíveis e operacionais sempre que necessário, garantindo a continuidade das atividades da ONG. A disponibilidade é assegurada por meio de backups regulares, planos de recuperação de desastres e monitoramento contínuo dos servidores e da infraestrutura, minimizando interrupções e perdas de dados.

PRIVACIDADE

O tratamento de dados pessoais (como os de pessoas atendidas, voluntários e parceiros) deve estar em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis. Isso garante a finalidade, a necessidade, a transparência e o consentimento no uso das informações, respeitando os direitos dos titulares dos dados.



GERENCIAMENTO DE ACESSO

Controle de Acesso

Todos os usuários do sistema e da infraestrutura da ONG devem possuir credenciais individuais e intransferíveis. Os níveis de acesso devem ser diferenciados e concedidos estritamente com base na função e necessidade (ex: usuário comum, administrador). O princípio do privilégio mínimo deve ser aplicado, concedendo aos usuários apenas o acesso e as permissões essenciais para desempenhar suas funções. O acesso ao sistema e banco de dados deve ser controlado, monitorado e revisado periodicamente

Autenticação

O sistema deve exigir login com senha forte e adotar práticas como expiração de sessão e uso de autenticação baseada em sessão segura. Recomenda-se a implementação de autenticação multifator (MFA) para acessos privilegiados, como administradores do sistema ou acesso a servidores. As senhas devem ser complexas (mínimo de 12 caracteres, combinando letras maiúsculas e minúsculas, números e símbolos) e únicas, não sendo reutilizadas em outros serviços ou plataformas.

Autorização

Usuários só podem executar operações e acessar funcionalidades conforme as permissões explicitamente concedidas ao seu perfil (ex.: apenas administradores podem excluir dados). Isso

evita o uso indevido de funcionalidades críticas do sistema. As permissões devem ser revisadas sempre que houver mudança de função, desligamento de um colaborador ou voluntário, ou periodicamente para garantir que estejam sempre adequadas.

SEGURANÇA FÍSICA E AMBIENTAL

Proteção de Instalações

Servidores, equipamentos de rede e computadores que armazenam ou processam dados da ONG devem ser mantidos em ambientes controlados e seguros, protegidos contra acesso não autorizado, roubo, danos e desastres físicos (como incêndios, inundações, falhas elétricas, etc.).

Controle de Acesso Físico

Apenas pessoas devidamente autorizadas devem ter acesso ao ambiente físico onde se localizam os servidores e equipamentos críticos, especialmente em ambientes de produção. O acesso a essas áreas deve ser registrado e monitorado por meio de logs de entrada e saída, câmeras de segurança ou outros sistemas de controle de acesso físico.

Segurança Ambiental

Os ambientes que abrigam servidores dedicados devem contar com infraestrutura adequada, como estabilizadores, nobreaks (para garantir energia contínua), sistemas de refrigeração eficientes para manter a temperatura ideal e detecção de incêndio. Sistemas de supressão de incêndio (ex: gás inerte) e monitoramento de temperatura e umidade devem ser considerados para infraestruturas mais críticas.

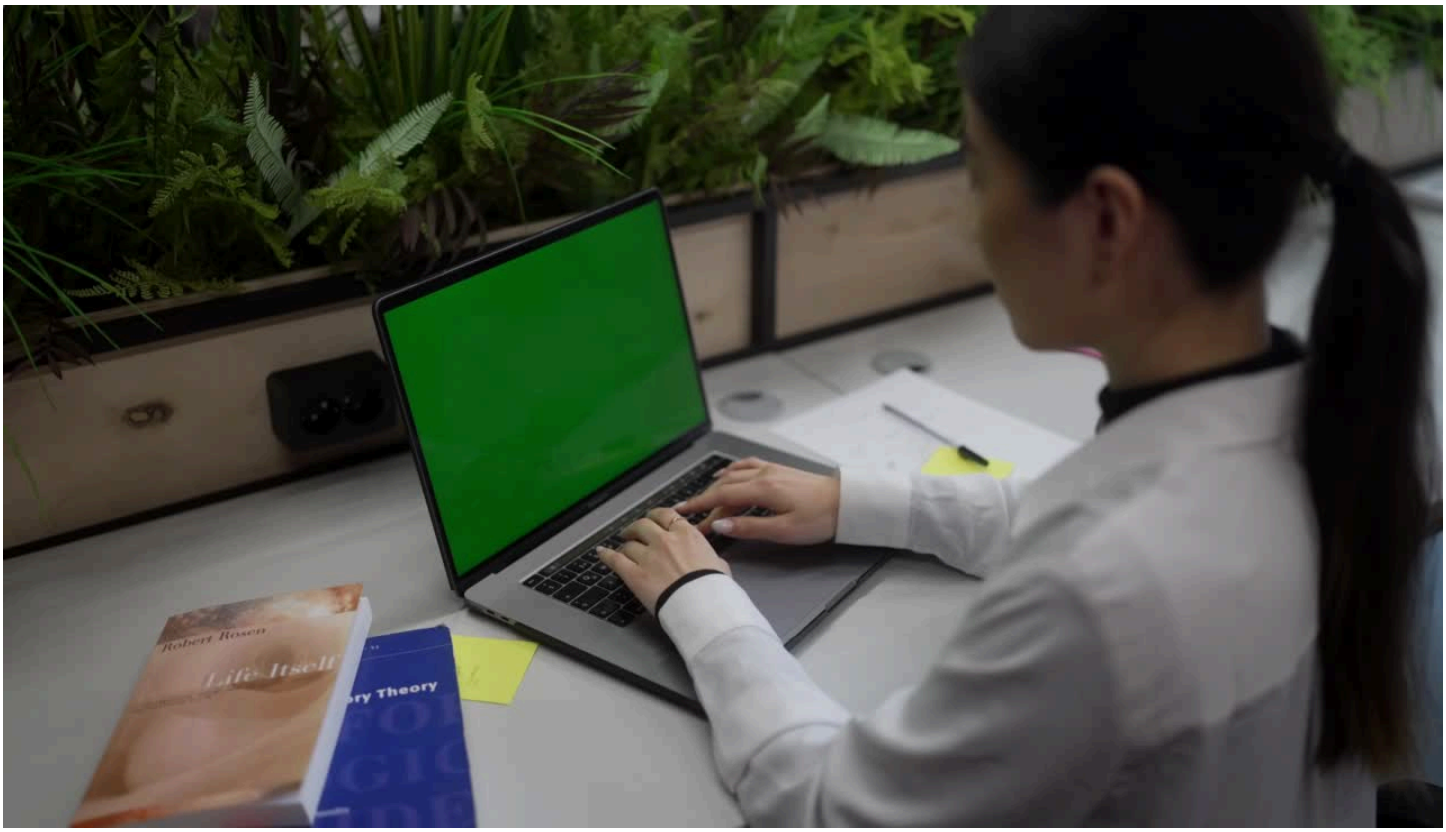
SEGURANÇA DE REDES E COMUNICAÇÕES

Proteção de Redes

É obrigatório o uso de firewalls para controlar o tráfego de rede, restrição de portas (ex: permitir apenas portas 22 para SSH, 80 para HTTP e 443 para HTTPS). O uso de HTTPS com certificados SSL/TLS é mandatório para todas as comunicações sensíveis e acesso ao sistema, garantindo a criptografia dos dados em trânsito. Medidas de proteção contra ataques de Negação de Serviço Distribuída (DDoS) devem ser implementadas. Recomenda-se a segmentação da rede para isolar sistemas críticos e dados sensíveis.

Monitoramento e Detecção de Intrusões

Devem ser implementados e revisados regularmente logs de acesso e erro do sistema e dos servidores. Ferramentas de monitoramento (como AWS CloudWatch para ambientes em nuvem) e alertas para atividades suspeitas, tentativas de acesso não autorizado ou anomalias de comportamento devem ser configurados. A implementação de Sistemas de Detecção de Intrusões (IDS) e Prevenção de Intrusões (IPS) deve ser considerada para maior proteção.



GESTÃO DE INCIDENTES DE SEGURANÇA

Resposta a Incidentes

Deve existir um procedimento de resposta rápida e documentado para incidentes de segurança. Este procedimento deve incluir etapas claras de identificação, contenção (isolamento do sistema ou ativos afetados), investigação, erradicação (mitigação da causa raiz), recuperação dos serviços e lições aprendidas. O plano de resposta a incidentes deve ser testado e revisado periodicamente.

Relatórios de Incidentes

Todos os incidentes de segurança, por menores que sejam, devem ser documentados e reportados à equipe responsável para análise posterior. Os relatórios devem incluir detalhes como data, hora, natureza do incidente, sistemas afetados, ações tomadas, impacto e medidas preventivas para evitar recorrências.

Comunicação de Incidentes

A comunicação de incidentes deve ser clara, transparente e realizada de forma oportuna. Internamente, deve-se informar as partes relevantes da equipe. Externamente, quando exigido legalmente (ex: LGPD), as autoridades competentes (ANPD) e as partes afetadas pelos dados devem ser notificadas em prazos estabelecidos

CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA

Programa de Conscientização

Um programa contínuo de conscientização sobre segurança da informação deve ser estabelecido. Usuários, desenvolvedores, administradores e voluntários devem ser constantemente informados sobre a importância da segurança da informação e seus papéis individuais na proteção dos dados da ONG. Este programa deve abordar os riscos específicos enfrentados pela ONG e as melhores práticas para mitigá-los

Treinamento em Segurança

Treinamentos periódicos e obrigatórios devem ser realizados para todos os membros da equipe e voluntários. O conteúdo deve incluir: uso seguro do sistema, boas práticas na criação e gestão de senhas, identificação de ataques comuns (como *phishing*, *malware*), manuseio seguro de dados pessoais e o entendimento e cumprimento das políticas de segurança da organização. Novos colaboradores e voluntários devem receber este treinamento como parte de sua integração.

AVALIAÇÃO E MELHORIA CONTÍNUA

Auditorias de Segurança

Auditorias de segurança regulares devem ser realizadas no código-fonte do sistema, na configuração do banco de dados e na infraestrutura tecnológica. Estas auditorias são especialmente importantes após grandes atualizações ou mudanças significativas. Recomenda-se a contratação de especialistas externos para realizar testes de penetração (*pentests*) e varreduras de vulnerabilidade independentes.

Análise de Riscos

Análises de risco periódicas devem ser conduzidas para identificar, avaliar e tratar as vulnerabilidades e ameaças à segurança da informação da ONG. Os resultados dessas análises devem guiar a implementação de medidas de segurança adicionais e a priorização de investimentos em segurança.

Revisão de Políticas e Procedimentos

As políticas e procedimentos de segurança da informação devem ser revisados e atualizados anualmente ou após qualquer incidente grave de segurança. O objetivo é incorporar novas ameaças identificadas, tecnologias emergentes, soluções atualizadas e mudanças regulatórias, garantindo a contínua relevância e eficácia da política. A revisão deve ser um processo colaborativo, envolvendo a equipe de TI (ou responsável pela segurança) e a direção da ONG.

Medição de Desempenho

Métricas de desempenho (KPIs) relacionadas à segurança devem ser monitoradas e avaliadas regularmente. Exemplos incluem: tempo médio de resposta a incidentes, número de acessos não autorizados bloqueados, frequência de backups bem-sucedidos, percentual de patches de segurança aplicados dentro do prazo e taxa de participação nos treinamentos de segurança.

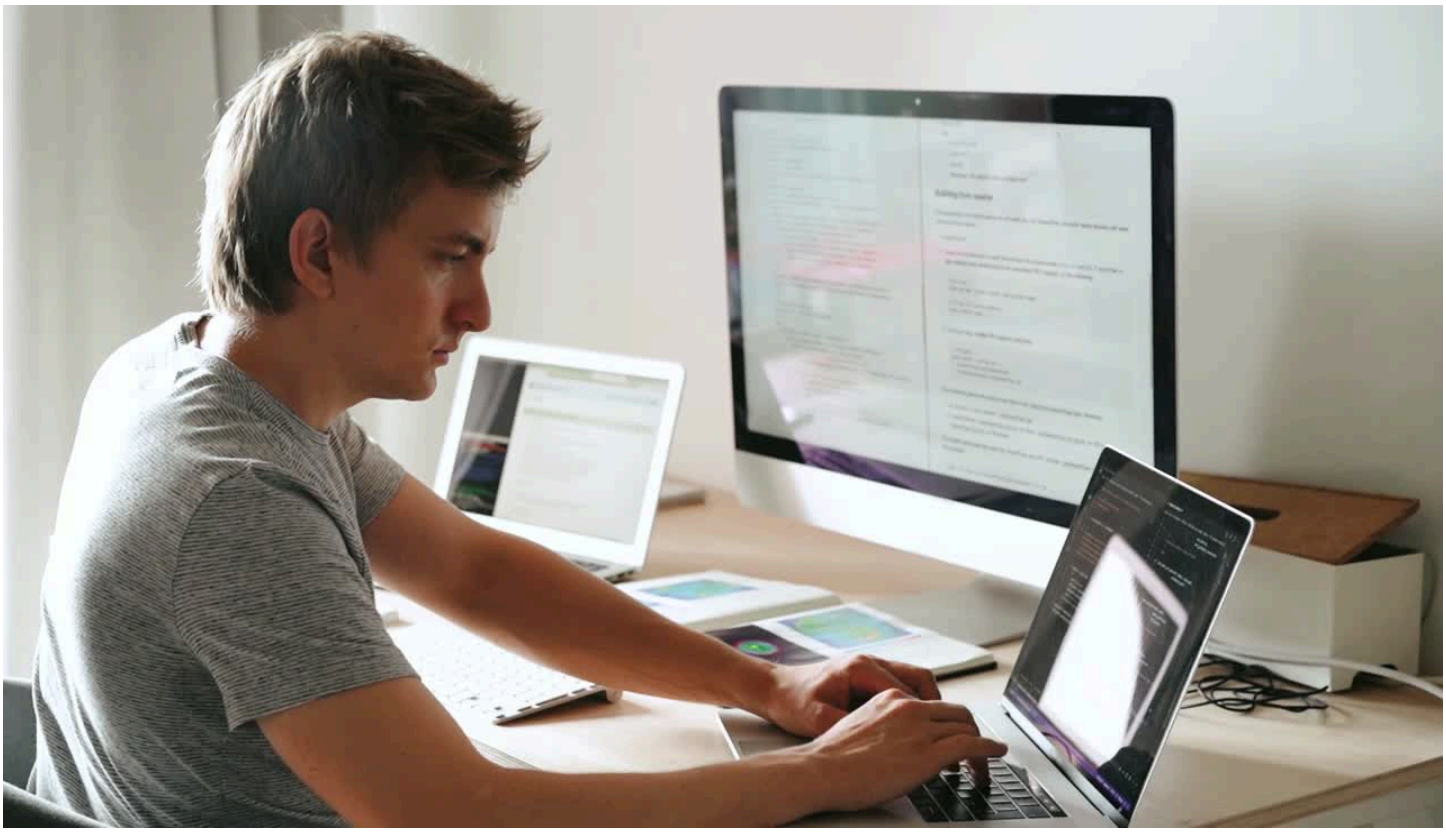
CONFORMIDADE LEGAL E REGULATÓRIA

Conformidade com Leis e Regulamentações

A ONG Solidariedade está comprometida em seguir rigorosamente a Lei Geral de Proteção de Dados (LGPD) e todas as demais leis e regulamentações aplicáveis ao tratamento de dados pessoais no Brasil. Isso inclui, mas não se limita a: obter o consentimento adequado dos titulares de dados, garantir os direitos dos titulares (acesso, correção, exclusão), e notificar a Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidentes de segurança graves, quando exigido por lei.

Gerenciamento de Vulnerabilidades e Patches

É crucial manter o sistema "ONG Solidariedade", o ambiente de desenvolvimento (XAMPP – se ainda utilizado para fins específicos), o PHP e o MySQL sempre atualizados com os últimos *patches* de segurança. Um processo formal de gerenciamento de *patches* e vulnerabilidades deve ser estabelecido para identificar, avaliar e aplicar as correções de segurança de forma proativa e tempestiva.



RESPONSABILIDADES

A segurança da informação é uma responsabilidade compartilhada por todos na ONG Solidariedade.

Direção da ONG

- Garantir a alocação de recursos financeiros e humanos necessários para a implementação e manutenção da segurança da informação.
- Oferecer apoio institucional e priorizar as iniciativas de segurança.
- Aprovar as políticas e procedimentos de segurança da informação.
- Promover e incentivar uma cultura de segurança em toda a organização.

Equipe de Tecnologia da Informação (ou Indivíduo Responsável pela Segurança)

- Implementar, monitorar e revisar continuamente as políticas e procedimentos de segurança.
- Realizar backups de dados e auditorias técnicas regulares.
- Gerenciar incidentes de segurança e aplicar as medidas corretivas.
- Manter-se atualizado sobre as melhores práticas de segurança, novas tecnologias e ameaças.
- Garantir a aplicação de *patches* e atualizações de segurança.

Funcionários e Voluntários

- Compreender e seguir rigorosamente todas as políticas e procedimentos de segurança da informação estabelecidos.
- Manter a confidencialidade de suas credenciais de acesso (senhas) e nunca compartilhá-las.
- Reportar imediatamente qualquer comportamento suspeito, tentativa de fraude, e-mail de *phishing* ou incidente de segurança à equipe responsável.
- Participar ativamente de todos os treinamentos e programas de conscientização em segurança.
- Utilizar os recursos tecnológicos da ONG de forma ética, responsável e em conformidade com esta política.

Versão e Aprovação:

Versão: 1.1

Data de Criação: 04 de Junho de 2025

Última Revisão: 04 de Junho de 2025

Elaborado por: Turma 02 - Eixo 5 - PucMinas (Rhafael Hector, Gustavo Gino, Thiago Ferreira, Natã Gabriel, Guilherme Alves, André Ramos, Isabella Carolina)

Aprovado por: Direção da ONG Solidariedade