

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO


<b>1. Introdução</b>	4
<b>2. Objetivos</b>	5
2.1. Garantir a Confidencialidade	5
2.2. Assegurar a Integridade	5
2.3. Manter a Disponibilidade	5
2.4. Conformidade com Leis e Regulamentos	5
2.5. Proteção contra Ameaças	5
2.6. Gestão de Riscos	6
2.7. Educação e Conscientização	6
2.8. Proteção de Dados Pessoais	6
2.9. Melhoria Contínua	6
2.10. Sustentabilidade Operacional	6
<b>3. Responsabilidades</b>	6
3.1. Diretoria Executiva	7
3.2. Gerente de TI	7
3.3. Equipe de TI	7
3.4. Gestores de Departamento	7
3.5. Usuários (Funcionários, Voluntários e Prestadores de Serviços)	8
3.6. Comitê de Segurança da Informação	8
3.7. Auditores Internos	8
3.8. Consultores Externos	8
<b>4. Classificação da Informação</b>	9
4.1. Confidencial	9
4.2. Interna	9
4.3. Pública	10
<b>5. Disposições gerais</b>	10
5.1. Internet	10
5.2. Recurso de correio eletrônico (e-mail)	10
5.3. Redes sem fio (Wi-Fi)	11

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

5.4. Recursos de TI institucionais .....	11
5.5. Recursos de TI particulares .....	11
5.6. Mídias sociais .....	11
5.7. Uso de áudio, vídeos e fotos .....	11
<b>6. Controle de Acesso .....</b>	<b>12</b>
6.1. Princípio do Menor Privilégio .....	12
6.2. Autenticação .....	12
6.3. Autorização .....	12
6.4. Controle de Acesso Físico .....	12
6.5. Monitoramento e Auditoria .....	13
6.6. Gestão de Contas .....	13
6.7. Segregação de Funções .....	13
6.8. Acesso Remoto .....	13
<b>7. Proteção de dados .....</b>	<b>13</b>
7.1. Criptografia .....	14
7.2. <i>Backup</i> e Recuperação de Dados .....	14
7.3. Controle de Acesso .....	14
7.4. Descarte Seguro de Dados .....	14
7.5. Proteção Contra Malware e Ameaças Cibernéticas.....	15
7.6. Privacidade e Conformidade com a LGPD.....	15
7.7. Acordos de Confidencialidade .....	15
<b>8. Segurança da informação .....</b>	<b>15</b>
8.1. <i>Firewall</i> .....	16
8.2. Segurança de Perímetro .....	16
8.3. Criptografia de Dados .....	16
8.4. Controle de Acesso à Rede (NAC) .....	16
8.5. Atualizações e <i>Patches</i> .....	16
8.6. Proteção contra <i>Malware</i> .....	17
8.7. Segurança Física .....	17
<b>9. Gestão de incidentes .....</b>	<b>17</b>
9.1. Definição de Incidentes .....	17

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

9.2. Detecção e Notificação .....	17
9.3. Avaliação e Análise .....	18
9.4. Resposta e Mitigação .....	18
9.5. Comunicação e Notificação .....	18
9.6. Documentação e Relatório .....	18
9.7. Equipe de Resposta a Incidentes .....	18
Revisão e Melhoria Contínua .....	19
<b>10. Revisão e auditoria .....</b>	<b>19</b>
10.1. Auditorias Internas Regulares .....	19
10.2. Avaliação de Conformidade .....	19
10.3. Testes de Penetração e Vulnerabilidade .....	20
10.4. Revisão de Políticas e Procedimentos .....	20
10.5. Avaliação de Controles Técnicos .....	20
10.6. Avaliação de Conscientização e Treinamento .....	20
10.7. Análise de Incidentes Anteriores .....	20
10.8. Relatórios e Recomendações .....	21
10.9. Acompanhamento e Implementação de Recomendações .....	21
10.10. Melhoria Contínua do Processo de Auditoria .....	21
<b>11. Penalidades de violação da política de segurança da informação .</b>	<b>21</b>
11.1. Ações Disciplinares: .....	21
11.2. Restrições de Acesso: .....	22
11.3. Responsabilidade Legal: .....	22
11.4. Educação e Conscientização Adicionais: .....	22
11.5. Perda de Privilégios: .....	22
11.6. Sanções Financeiras: .....	22
11.7. Revisão das Políticas e Procedimentos: .....	23
11.8. Comunicação Interna: .....	23
<b>12. Considerações finais .....</b>	<b>23</b>

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

## 1. Introdução


A segurança da informação é um componente crítico para a proteção dos ativos digitais e físicos de qualquer organização, incluindo as organizações não governamentais (ONGs), que frequentemente lidam com dados sensíveis de beneficiários, doadores e parceiros. No contexto atual, onde as ameaças cibernéticas estão em constante evolução, garantir a integridade, confidencialidade e disponibilidade das informações tornou-se indispensável.

Esta Política de Segurança da Informação foi desenvolvida para o Departamento de TI da ONG com o objetivo de estabelecer diretrizes claras e práticas que assegurem a proteção das informações e sistemas de informação da organização. Ao implementar esta política, busca-se não apenas cumprir com as exigências legais e regulamentares, mas também reforçar a confiança de todos os stakeholders que confiam na ONG para conduzir suas atividades de maneira segura e responsável.

A política está alinhada com a norma ABNT NBR ISO/IEC 27001, que estabelece requisitos para um sistema de gestão de segurança da informação (SGSI). Esta norma fornece uma abordagem sistemática para gerenciar informações sensíveis, garantindo sua segurança por meio da avaliação e tratamento de riscos, implementação de controles de segurança específicos e criação de uma estrutura organizacional robusta para a gestão de segurança da informação. A conformidade com a ABNT NBR ISO/IEC 27001 é uma evidência do compromisso da ONG com as melhores práticas de segurança da informação reconhecidas internacionalmente.

Reconhece-se que a segurança da informação é uma responsabilidade coletiva que requer a colaboração de todos os membros da ONG, desde a diretoria até os voluntários. Esta política detalha as responsabilidades de cada grupo dentro da organização, as medidas de segurança que devem ser adotadas, e os procedimentos para gerenciar incidentes de segurança. Além disso, enfatiza-se a importância de uma cultura de conscientização e de treinamento contínuo para todos os envolvidos.

Com esta política, a ONG reafirma seu compromisso em proteger as informações e em operar de maneira ética e segura, garantindo que suas

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

atividades possam continuar a beneficiar aqueles a quem serve, sem comprometer a segurança e a privacidade dos dados.

## 2. Objetivos

A política de segurança da informação da ONG visa alcançar os seguintes objetivos fundamentais:

### 2.1. Garantir a Confidencialidade

- Proteger informações sensíveis contra acessos não autorizados.
- Assegurar que apenas pessoas autorizadas tenham acesso a dados confidenciais.

### 2.2. Assegurar a Integridade

- Manter a precisão e a completude das informações e dos sistemas de processamento de dados.
- Prevenir alterações não autorizadas nos dados, seja acidental ou intencionalmente.

### 2.3. Manter a Disponibilidade


- Garantir que as informações e os sistemas de informação estejam disponíveis para uso quando necessário.
- Minimizar o tempo de inatividade e assegurar a continuidade das operações.

### 2.4. Conformidade com Leis e Regulamentos

- Assegurar que todas as práticas de segurança da informação estejam em conformidade com as leis e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD).
- Atender aos requisitos de regulamentações específicas do setor e normas internacionais, como a ABNT NBR ISO/IEC 27001.

### 2.5. Proteção contra Ameaças

- Implementar medidas para identificar, prevenir e responder a ameaças cibernéticas.
- Proteger a organização contra-ataques cibernéticos, vazamentos de dados, malware e outras ameaças de segurança.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

## 2.6. Gestão de Riscos

- Realizar avaliações contínuas de risco para identificar vulnerabilidades e implementar controles adequados.
- Desenvolver e manter um plano de resposta a incidentes para lidar com potenciais violações de segurança.

## 2.7. Educação e Conscientização

- Promover uma cultura de segurança da informação entre todos os membros da ONG.
- Oferecer treinamentos regulares e campanhas de conscientização para garantir que todos compreendam a importância da segurança da informação e saibam como proteger os dados.

## 2.8. Proteção de Dados Pessoais

- Assegurar que os dados pessoais dos beneficiários, doadores, voluntários e funcionários sejam tratados com respeito e protegidos contra usos indevidos.
- Implementar medidas para garantir a privacidade e a segurança dos dados pessoais conforme as melhores práticas e normas vigentes.

## 2.9. Melhoria Contínua


- Monitorar e revisar continuamente as práticas e políticas de segurança da informação para garantir sua eficácia.
- Implementar melhorias contínuas baseadas em novas ameaças, tecnologias emergentes e lições aprendidas de incidentes passados.

## 2.10. Sustentabilidade Operacional

- Assegurar que a segurança da informação suporte a missão e os objetivos estratégicos da ONG.
- Alinhar as práticas de segurança da informação com os valores e metas da organização para garantir a sustentabilidade a longo prazo.

## 3. Responsabilidades

Para garantir a eficácia da Política de Segurança da Informação, é essencial que todas as partes envolvidas entendam e cumpram suas

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

responsabilidades. Abaixo estão definidas as responsabilidades de cada grupo dentro da organização:

### 3.1. Diretoria Executiva

- Aprovar e apoiar a implementação desta política.
- Alocar recursos necessários para a implementação e manutenção das medidas de segurança da informação.
- Promover uma cultura organizacional que valorize a segurança da informação.


### 3.2. Gerente de TI

- Desenvolver, implementar e manter a Política de Segurança da Informação.
- Realizar avaliações de risco periódicas e implementar controles adequados.
- Monitorar a conformidade com a política e relatar o status à diretoria.
- Coordenar a resposta a incidentes de segurança e a recuperação de desastres.
- Garantir que todos os sistemas de informação estejam devidamente protegidos contra ameaças.
- Supervisionar a aplicação de controles de acesso e garantir que as permissões estejam alinhadas com as funções e responsabilidades dos usuários.
- Realizar treinamentos de segurança da informação para todos os funcionários e voluntários.

### 3.3. Equipe de TI

- Implementar e manter os controles de segurança da informação conforme definido na política.
- Monitorar a rede e os sistemas de informação para detectar e responder a ameaças.
- Gerenciar a segurança física dos equipamentos de TI.
- Realizar backups regulares e garantir que os dados possam ser recuperados em caso de incidente.
- Assegurar que todos os dispositivos estejam atualizados com os patches de segurança mais recentes.
- Documentar e relatar incidentes de segurança ao Gerente de TI.

### 3.4. Gestores de Departamento

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Garantir que suas equipes compreendam e cumpram a Política de Segurança da Informação.
- Colaborar com a equipe de TI para identificar e mitigar riscos específicos do departamento.
- Relatar quaisquer incidentes de segurança ou suspeitas de violações à equipe de TI imediatamente.

### 3.5. Usuários (Funcionários, Voluntários e Prestadores de Serviços)

- Cumprir todas as diretrizes e procedimentos de segurança da informação estabelecidos na política.
- Usar senhas fortes e mantê-las confidenciais.
- Relatar imediatamente quaisquer incidentes de segurança ou atividades suspeitas à equipe de TI.
- Participar dos treinamentos e programas de conscientização de segurança da informação.
- Manter a confidencialidade das informações acessadas durante suas atividades na ONG.
- Seguir as práticas recomendadas para o descarte seguro de informações sensíveis.

### 3.6. Comitê de Segurança da Informação

- Realizar revisões periódicas da Política de Segurança da Informação.
- Avaliar a eficácia dos controles de segurança e sugerir melhorias.
- Promover a conscientização sobre segurança da informação em toda a organização.
- Supervisionar a conformidade com as normas e regulamentações aplicáveis.


### 3.7. Auditores Internos

- Conduzir auditorias regulares para garantir a conformidade com a Política de Segurança da Informação.
- Identificar e reportar vulnerabilidades e não-conformidades.
- Recomendar melhorias baseadas nos achados das auditorias.

### 3.8. Consultores Externos

- Oferecer expertise em segurança da informação e apoiar na implementação de melhores práticas.
- Realizar avaliações independentes e testes de penetração para identificar vulnerabilidades.



	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Fornecer treinamento especializado e capacitação para a equipe de TI.

#### 4. Classificação da Informação

Para garantir a segurança e a adequada proteção das informações, todas as informações manejadas pela ONG serão classificadas em três categorias principais, baseadas em seu nível de sensibilidade e necessidade de proteção:

##### 4.1. Confidencial

Informações que, se divulgadas sem autorização, podem causar dano significativo à ONG, seus beneficiários, doadores, parceiros ou funcionários. O acesso a estas informações é estritamente limitado a indivíduos autorizados.

Exemplos:

- Dados pessoais de beneficiários (ex.: informações de saúde, dados financeiros).
- Dados pessoais de funcionários e voluntários (ex.: CPF, endereços, dados bancários).
- Documentos estratégicos da ONG (ex.: planos de negócios, estratégias de captação de recursos).
- Informações financeiras e contábeis confidenciais.
- Contratos e acordos com parceiros e fornecedores.
- Informações sobre doadores e suas doações.

Medidas de Proteção:


- Criptografia em repouso e em trânsito.
- Controle de acesso rigoroso, baseado na necessidade de conhecimento.
- Backup seguro e armazenamento em locais seguros.
- Descarte seguro, como trituração de documentos físicos e exclusão segura de arquivos digitais.

##### 4.2. Interna

Informações destinadas ao uso interno da ONG, que não são publicamente disponíveis, mas cuja divulgação não autorizada teria impacto moderado. Disponível para todos os funcionários e voluntários, mas não deve ser compartilhada fora da organização sem autorização.

Exemplos:

- Políticas e procedimentos internos.
- Relatórios de reuniões internas.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Comunicação interna (ex.: e-mails, memorandos).
- Dados operacionais não sensíveis.

Medidas de Proteção:

- Controle de acesso moderado.
- Senhas e autenticação para acesso a sistemas internos.
- Backup regular e medidas de segurança básicas.

#### 4.3. Pública

Informações que podem ser divulgadas sem restrições e cuja divulgação não causa danos à ONG, seus beneficiários, doadores, parceiros ou funcionários. Estas informações estão disponíveis para o público em geral.

Exemplos:

- Informações publicadas no site da ONG (ex.: missão, visão, valores, relatórios anuais).
- Comunicados de imprensa.
- Material de divulgação e campanhas publicitárias.
- Dados estatísticos e de impacto já divulgados.

Medidas de Proteção:

- Revisão e autorização antes da divulgação para garantir precisão.
- Monitoramento contínuo para evitar desinformação ou uso indevido.


## 5. Disposições gerais

### 5.1. Internet

- O uso da internet deve ser estritamente para fins comerciais relacionados às atividades da organização.
- Evitar o acesso a sites não seguros ou conteúdo inadequado que possa comprometer a segurança da informação.

### 5.2. Recurso de correio eletrônico (e-mail)

- O e-mail da organização deve ser usado apenas para fins comerciais legítimos.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Evitar o envio ou recebimento de e-mails não relacionados ao trabalho ou de conteúdo inadequado.

### 5.3. Redes sem fio (Wi-Fi)

- A ONG, quando possível, oferecem à comunidade administrativa, nos ambientes autorizados e limitados ao perímetro físico da instituição, uma rede sem fio (Wi-Fi) própria para finalidades administrativas.
- Somente os colaboradores expressamente autorizados podem ter acesso à rede sem fio (Wi-Fi) da instituição e devem comprometer-se a fazer uso seguro desse recurso.
- Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização do gestor imediato.

### 5.4. Recursos de TI institucionais

- Os recursos de TI institucionais devem ser usados apenas por funcionários autorizados para fins comerciais.

### 5.5. Recursos de TI particulares

- O uso de recursos de TI particulares na rede da organização deve ser autorizado e estar em conformidade com esta política.

### 5.6. Mídias sociais


- O uso de mídias sociais deve estar em conformidade com as diretrizes estabelecidas pela organização.

### 5.7. Uso de áudio, vídeos e fotos

- O uso de áudio, vídeos e fotos deve ser estritamente para fins comerciais relacionados às atividades da organização.

### 5.8. Limpeza e Organização do Ambiente de Trabalho

- Mantenha a mesa de trabalho limpa e organizada.
- Bloqueie a tela do computador sempre que se afastar da mesa e armazene documentos físicos de maneira segura.
- Descarte documentos confidenciais, utilizando serviços de destruição apropriados.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

## 6. Controle de Acesso

O controle de acesso é um componente fundamental da Política de Segurança da Informação da ONG, garantindo que apenas indivíduos autorizados possam acessar informações e sistemas de acordo com suas responsabilidades e necessidades. A seguir estão detalhados os mecanismos e práticas de controle de acesso que serão implementados:

### 6.1. Princípio do Menor Privilégio

Todos os usuários receberão o nível mínimo de acesso necessário para realizar suas funções. Este princípio minimiza a exposição de informações sensíveis e reduz o risco de acesso não autorizado.

### 6.2. Autenticação

**Senhas Fortes:** Todos os usuários devem utilizar senhas complexas que atendam aos seguintes critérios:


- Mínimo de 8 caracteres.
- Incluindo letras maiúsculas e minúsculas, números e caracteres especiais.
- Autenticação Multifator (MFA): Implementar MFA para acessos críticos, garantindo uma camada adicional de segurança além das senhas.
- Política de Troca de Senhas: As senhas devem ser trocadas regularmente, pelo menos a cada 90 dias, e nunca reutilizadas.

### 6.3. Autorização

- Perfis de Acesso: Os perfis de acesso são baseados em funções, garantindo que os usuários tenham acesso apenas aos recursos necessários para suas funções específicas.
- Revisão de Acessos: Realizar revisões periódicas dos acessos concedidos para assegurar que apenas as pessoas apropriadas mantenham seus privilégios.

### 6.4. Controle de Acesso Físico

- Áreas Restritas: As áreas com sistemas de informação sensíveis devem ser fisicamente protegidas, acessíveis apenas a pessoal autorizado.
- Cartões de Acesso e Biometria: Utilizar cartões de acesso ou sistemas biométricos para controlar a entrada em áreas restritas.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

#### 6.5. Monitoramento e Auditoria

- Logs de Acesso: Manter logs detalhados de todas as tentativas de acesso aos sistemas e informações sensíveis, incluindo sucesso e falha.
- Monitoramento Contínuo: Implementar ferramentas de monitoramento contínuo para detectar e alertar sobre atividades suspeitas ou anômalas.
- Auditorias Periódicas: Realizar auditorias periódicas para revisar os logs de acesso e garantir a conformidade com a política de controle de acesso.

#### 6.6. Gestão de Contas

- Criação e Desativação de Contas: Contas de usuário devem ser criadas, modificadas e desativadas conforme a entrada, movimentação e saída de funcionários e voluntários, assegurando que os acessos sejam apropriados ao status do usuário.
- Acesso Temporário: Acessos temporários devem ser concedidos somente quando necessário e devem ter uma validade predeterminada.

#### 6.7. Segregação de Funções


- Divisão de Responsabilidades: Assegurar que nenhuma pessoa tenha controle total sobre todas as fases de uma transação ou processo sensível, minimizando riscos de fraude e erros.

#### 6.8. Acesso Remoto

- VPN Segura: O acesso remoto aos sistemas da ONG é realizado exclusivamente através de uma rede privada virtual (VPN) segura e autenticada.
- Políticas de BYOD (*Bring Your Own Device*): Estabelecer políticas claras para o uso de dispositivos pessoais, incluindo requisitos de segurança e conformidade com as normas da ONG.

### 7. Proteção de dados

A proteção de dados é um aspecto crítico da segurança da informação, especialmente para uma ONG que lida com dados sensíveis de beneficiários, doadores, parceiros e funcionários. A seguir estão detalhadas as medidas que nossa ONG implementará para garantir a proteção adequada dos dados:

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

### 7.1. Criptografia

- **Dados em Repouso:** Todos os dados sensíveis devem ser criptografados quando armazenados em servidores, dispositivos de armazenamento e backups.
- **Dados em Trânsito:** A criptografia deve ser usada para proteger dados durante a transmissão, usando protocolos seguros como SSL/TLS.
- **Chaves Criptográficas:** As chaves criptográficas devem ser gerenciadas de forma segura, com acesso restrito e práticas de rotação regular.

### 7.2. Backup e Recuperação de Dados


- **Backups Regulares:** Realizar *backups* regulares dos dados importantes, garantindo que cópias de segurança sejam armazenadas em locais seguros.
- **Armazenamento de Backups:** Backups devem ser armazenados em locais separados fisicamente e logicamente do local original dos dados.
- **Teste de Recuperação:** Realizar testes periódicos de recuperação de dados para garantir que os *backups* possam ser restaurados com sucesso em caso de necessidade.

### 7.3. Controle de Acesso

- **Autenticação e Autorização:** Implementar controles rigorosos de autenticação e autorização para garantir que apenas usuários autorizados possam acessar dados sensíveis.
- **Segregação de Funções:** Garantir que funções e responsabilidades sejam segregadas para prevenir acesso não autorizado e fraudes.
- **Monitoramento de Acesso:** Manter registros detalhados de acessos a dados sensíveis e revisar regularmente esses registros para detectar atividades suspeitas.

### 7.4. Descarte Seguro de Dados

- **Dados Digitais:** Implementar procedimentos seguros para a exclusão de dados digitais, como o uso de software de exclusão segura que impede a recuperação de dados.
- **Documentos Físicos:** Utilizar métodos seguros para o descarte de documentos físicos, como trituração, para garantir que informações confidenciais não possam ser recuperadas.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

#### 7.5. Proteção Contra Malware e Ameaças Cibernéticas

- **Antivírus e Antimalware:** Utilizar software antivírus e *antimalware* atualizado em todos os dispositivos e servidores.
- **Firewalls:** Implementar *firewalls* para proteger a rede contra acessos não autorizados e ataques externos.
- **Atualizações e Patches:** Manter todos os sistemas e aplicativos atualizados com os *patches* de segurança mais recentes.

#### 7.6. Privacidade e Conformidade com a LGPD


- **Política de Privacidade:** Estabelecer e comunicar uma política de privacidade que descreva como os dados pessoais são coletados, usados, armazenados e protegidos.
- **Consentimento Informado:** Obter consentimento explícito dos indivíduos antes de coletar e processar seus dados pessoais, conforme exigido pela Lei Geral de Proteção de Dados (LGPD).
- **Direitos dos Titulares:** Assegurar que os titulares dos dados possam exercer seus direitos, como acesso, correção, exclusão e portabilidade de seus dados pessoais.
- **Relatórios e Auditorias:** Realizar auditorias regulares para garantir a conformidade com a LGPD e outras regulamentações de privacidade.

#### 7.7. Acordos de Confidencialidade

- **Funcionários e Voluntários:** Exigir que todos os funcionários e voluntários assinem acordos de confidencialidade para proteger informações sensíveis.
- **Terceiros e Parceiros:** Estabelecer contratos de confidencialidade com terceiros e parceiros que possam ter acesso a dados sensíveis, garantindo o cumprimento das normas de proteção de dados da ONG.

### 8. Segurança da informação

A segurança de rede é essencial para proteger as informações e garantir a integridade e disponibilidade dos sistemas de informação da ONG. As medidas de segurança de rede descritas abaixo visam prevenir acessos não autorizados, ataques cibernéticos e outras ameaças, assegurando a operação contínua e segura da organização.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

### 8.1. Firewall

- Implementação de *Firewall*: Utilizar *firewalls* para controlar o tráfego de rede entre a rede interna da ONG e redes externas, como a internet. Os *firewalls* devem ser configurados para bloquear acessos não autorizados e permitir apenas tráfego legítimo.
- Regras de *Firewall*: Estabelecer e revisar regularmente regras de *firewall* para garantir que apenas o tráfego necessário seja permitido.

### 8.2. Segurança de Perímetro

- IDS/IPS: Implementar sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar e analisar o tráfego de rede em busca de atividades suspeitas e ataques em potencial.
- Segmentação de Rede: Segmentar a rede interna em diferentes zonas de segurança, isolando sistemas críticos e dados sensíveis para limitar o impacto de um possível incidente.

### 8.3. Criptografia de Dados

- VPN: Utilizar redes privadas virtuais (VPNs) para proteger dados em trânsito entre dispositivos remotos e a rede da ONG. As VPNs devem usar protocolos de criptografia robustos para garantir a confidencialidade e integridade dos dados.
- Wi-Fi Seguro: Configurar redes Wi-Fi internas com criptografia WPA3 e senhas fortes. Redes Wi-Fi para convidados devem ser separadas da rede principal da ONG.


### 8.4. Controle de Acesso à Rede (NAC)

- Autenticação: Implementar mecanismos de autenticação forte para acessar a rede, como autenticação multifator (MFA).
- Acesso Baseado em Funções: Utilizar controles de acesso baseados em funções (RBAC) para garantir que os usuários tenham acesso apenas aos recursos necessários para suas funções específicas.

### 8.5. Atualizações e Patches

- Gerenciamento de *Patches*: Manter todos os dispositivos de rede, sistemas operacionais e aplicativos atualizados com os *patches* de segurança mais recentes.



	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- **Automatização:** Automatizar o processo de atualização de software sempre que possível para garantir que as correções sejam aplicadas prontamente.

#### 8.6. Proteção contra *Malware*

- **Antivírus e *Antimalware*:** Implementar software antivírus e *antimalware* em todos os dispositivos conectados à rede e garantir que sejam atualizados regularmente.
- **Filtragem de Conteúdo:** Utilizar filtragem de conteúdo para bloquear sites maliciosos e impedir *downloads* de arquivos perigosos.

#### 8.7. Segurança Física

- **Proteção de Equipamentos de Rede:** Garantir que os equipamentos de rede (como roteadores, *switches* e servidores) estejam localizados em áreas seguras e com acesso restrito.
- **Monitoramento Físico:** Utilizar câmeras de vigilância e controles de acesso físico para proteger os locais onde estão os equipamentos de rede.

### 9. Gestão de incidentes


A gestão de incidentes é uma parte fundamental da Política de Segurança da Informação da ONG, visando identificar, responder e mitigar incidentes de segurança de forma eficaz para minimizar o impacto nos nossos sistemas e dados. A seguir estão detalhados os procedimentos e responsabilidades relacionados à gestão de incidentes:

#### 9.1. Definição de Incidentes

- **Classificação de Incidentes:** Identificar e documentar incidentes, incluindo acesso não autorizado, *malware*, *phishing*, violação de dados e interrupções de serviço.

#### 9.2. Detecção e Notificação

- **Mecanismos de Detecção:** Implementar sistemas de detecção de intrusões, monitoramento de rede e outras ferramentas para identificar incidentes de segurança o mais rápido possível.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- **Procedimentos de Notificação:** Estabelecer canais de comunicação claros e procedimentos para relatar incidentes à equipe de segurança da informação e à diretoria.

### 9.3. Avaliação e Análise

- **Investigação Preliminar:** Realizar uma análise inicial para determinar a natureza e a extensão do incidente.
- **Coleta de Evidências:** Coletar e preservar evidências relacionadas ao incidente, incluindo logs de sistema, registros de acesso e capturas de tela.

### 9.4. Resposta e Mitigação

- **Contenção:** Agir rapidamente para conter o incidente e evitar que se espalhe para outros sistemas ou áreas da organização.
- **Erradicação:** Identificar e remover completamente o malware, as vulnerabilidades ou as ameaças que causaram o incidente.
- **Recuperação:** Restaurar os sistemas afetados para um estado operacional normal, incluindo a recuperação de dados se necessário.

### 9.5. Comunicação e Notificação


- **Comunicação Interna:** Manter a equipe informada sobre o status do incidente e as medidas tomadas para responder e mitigar o impacto.
- **Notificação Externa:** Se necessário e conforme exigido por regulamentos, notificar autoridades regulatórias, parceiros ou clientes afetados pelo incidente.

### 9.6. Documentação e Relatório

- **Registro de Incidentes:** Documentar detalhadamente todos os aspectos do incidente, incluindo a cronologia dos eventos, as ações tomadas e as lições aprendidas.
- **Análise Pós-Incidente:** Realizar uma análise pós-incidente para identificar falhas no processo e áreas de melhoria.

### 9.7. Equipe de Resposta a Incidentes

- **Designação de Papéis:** Designar funções e responsabilidades específicas para os membros da equipe de resposta a incidentes, incluindo líderes de equipe, investigadores, analistas e comunicadores.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- **Treinamento Especializado:** Garantir que a equipe de resposta a incidentes receba treinamento especializado e tenha acesso às ferramentas e recursos necessários para realizar suas funções com eficácia.

#### Revisão e Melhoria Contínua

- **Avaliação Pós-Incidente:** Realizar revisões pós-incidente para avaliar a eficácia da resposta e identificar oportunidades de melhoria.
- **Atualização de Procedimentos:** Atualizar os procedimentos de gestão de incidentes com base nas lições aprendidas e nos resultados das análises pós-incidente.

### 10. Revisão e auditoria


A revisão e auditoria em segurança da informação são processos cruciais para garantir a eficácia das políticas, procedimentos e controles de segurança implementados pela ONG. Essas atividades permitem identificar possíveis vulnerabilidades, avaliar o cumprimento de normas e regulamentos, e fornecer recomendações para melhorias. Abaixo estão detalhadas as práticas de revisão e auditoria que serão adotadas:

#### 10.1. Auditorias Internas Regulares

- **Escopo Abrangente:** Realizar auditorias internas abrangentes para avaliar todos os aspectos da segurança da informação, incluindo políticas, procedimentos, controles técnicos e práticas de conformidade.
- **Plano de Auditoria:** Desenvolver um plano de auditoria anual que estabeleça os objetivos, escopo, métodos e cronograma das auditorias internas.

#### 10.2. Avaliação de Conformidade

- **Normas e Regulamentos:** Verificar o cumprimento das normas e regulamentos relevantes, como a Lei Geral de Proteção de Dados (LGPD), ISO/IEC 27001 e outras diretrizes específicas do setor.
- **Políticas Internas:** Comparar as práticas e procedimentos internos com as políticas de segurança da informação da organização para garantir alinhamento e conformidade.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

### 10.3. Testes de Penetração e Vulnerabilidade

- **Simulação de Ataques:** Realizar testes de penetração e avaliações de vulnerabilidade para identificar possíveis pontos fracos na infraestrutura de TI e nos sistemas da organização.
- **Remediação de Vulnerabilidades:** Tomar medidas corretivas imediatas para mitigar quaisquer vulnerabilidades identificadas durante os testes de penetração.

### 10.4. Revisão de Políticas e Procedimentos

- **Atualização Contínua:** Revisar regularmente as políticas e procedimentos de segurança da informação para garantir que estejam alinhados com as melhores práticas do setor e as mudanças nas necessidades e requisitos da organização.
- **Participação Multidisciplinar:** Envolvimento de diversas partes interessadas na revisão e atualização das políticas, incluindo a equipe de TI, a liderança executiva e os representantes de departamentos-chave.

### 10.5. Avaliação de Controles Técnicos


- **Eficácia dos Controles:** Avaliar a eficácia dos controles técnicos implementados para proteger os sistemas e dados da organização, como firewalls, sistemas de detecção de intrusões e antivírus.
- **Configurações Seguras:** Verificar se os dispositivos e sistemas estão configurados de acordo com as melhores práticas de segurança e as políticas da organização.

### 10.6. Avaliação de Conscientização e Treinamento

- **Participação e Conscientização:** Avaliar o nível de participação e conscientização dos funcionários e voluntários em relação às práticas de segurança da informação.
- **Eficácia do Treinamento:** Avaliar a eficácia dos programas de treinamento e conscientização em segurança da informação, medindo o impacto nas práticas de segurança dos participantes.

### 10.7. Análise de Incidentes Anteriores

- **Lições Aprendidas:** Analisar incidentes de segurança anteriores para identificar falhas nos controles de segurança e implementar medidas corretivas para evitar recorrências.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Melhoria Contínua: Utilizar as lições aprendidas com incidentes anteriores para melhorar continuamente as práticas de segurança da informação da organização.

#### 10.8. Relatórios e Recomendações

- Relatórios Abrangentes: Elaborar relatórios detalhados que destaquem as descobertas das revisões e auditorias, incluindo recomendações claras para melhorias.
- Comunicação Efetiva: Comunicar os resultados das revisões e auditorias de forma clara e objetiva à liderança executiva e às partes interessadas relevantes.

#### 10.9. Acompanhamento e Implementação de Recomendações

- Planos de Ação: Desenvolver planos de ação claros para implementar as recomendações identificadas durante as revisões e auditorias.
- Acompanhamento Regular: Acompanhar regularmente o progresso na implementação das recomendações e tomar medidas corretivas conforme necessário.

#### 10.10. Melhoria Contínua do Processo de Auditoria


- Feedback e Avaliação: Solicitar feedback das partes interessadas e participantes sobre o processo de auditoria para identificar áreas de melhoria.
- Atualização de Metodologias: Atualizar continuamente as metodologias de auditoria com base nas melhores práticas e nas mudanças no ambiente de segurança da informação.

### 11. Penalidades de violação da política de segurança da informação

As penalidades para violação da política de segurança podem variar dependendo da gravidade da violação, das políticas internas da organização e das leis e regulamentos aplicáveis. Abaixo estão algumas das possíveis penalidades que podem ser aplicadas:

#### 11.1. Ações Disciplinares:

- Advertência verbal ou escrita: Para violações menores ou de baixo impacto, uma advertência pode ser emitida para o funcionário infrator.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

- Suspensão temporária: Em casos mais graves, pode ser aplicada uma suspensão temporária do trabalho como consequência da violação da política.
- Demissão: Se a violação for significativa ou repetida, pode resultar em demissão do funcionário, especialmente se houver negligência grave ou intenção de causar danos.

#### 11.2. Restrições de Acesso:

- Revogação de privilégios de acesso: O acesso aos sistemas e dados da organização pode ser temporariamente ou permanentemente revogado como medida disciplinar.
- Restrição de funções: O funcionário infrator pode ter suas responsabilidades reduzidas ou limitadas como resultado da violação da política.

#### 11.3. Responsabilidade Legal:

- Ações legais: Em casos extremos, a violação da política de segurança pode levar a ações legais contra o funcionário infrator, especialmente se a violação resultar em danos significativos à organização ou a terceiros.

#### 11.4. Educação e Conscientização Adicionais:


- Treinamento adicional: Como parte da medida disciplinar, o funcionário infrator pode ser obrigado a participar de treinamentos adicionais sobre segurança da informação para aumentar a conscientização e prevenir violações futuras.

#### 11.5. Perda de Privilégios:

- Perda de benefícios ou privilégios: Dependendo da gravidade da violação, o funcionário infrator pode perder certos benefícios ou privilégios dentro da organização, como bonificações ou oportunidades de promoção.

#### 11.6. Sanções Financeiras:

- Multas internas: Em algumas organizações, pode haver a imposição de multas financeiras como consequência da violação da política de segurança da informação.
- Responsabilidade por danos: O funcionário infrator pode ser responsabilizado por quaisquer danos financeiros resultantes da violação, incluindo custos de remediação e perda de receita.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

#### 11.7. Revisão das Políticas e Procedimentos:

- Atualização das políticas: A violação da política pode levar à revisão e atualização das políticas e procedimentos de segurança da informação para prevenir violações futuras e fortalecer os controles de segurança.

#### 11.8. Comunicação Interna:

- Divulgação da violação: Dependendo da gravidade da violação, pode ser necessário comunicar a violação da política de segurança aos funcionários da organização para destacar a importância da conformidade.

## 12. Considerações finais

A segurança da informação é uma responsabilidade compartilhada por todos os membros da ONG. Ao seguir esta política e colaborar ativamente na proteção dos ativos de informação da organização, podemos garantir a confidencialidade, integridade e disponibilidade dos dados, além de promover uma cultura de segurança da informação em toda a organização.

Ademais, esta política será revisada regularmente para garantir sua eficácia contínua e para incorporar quaisquer mudanças nas leis, regulamentos ou nas necessidades da organização.

Data de Entrada em Vigor: 03/06/2024

Data de Revisão: 15/06/2024

Por fim, esta política de segurança da informação é parte integrante das práticas de governança da ONG e deve ser respeitada por todos os colaboradores, independentemente do cargo ou função que ocupam. O cumprimento destas diretrizes é essencial para manter a confiança dos beneficiários, doadores e parceiros, além de garantir a continuidade e a integridade das operações da organização.