	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão 1.0

Sumário

1 INTRODUÇÃO

A Quatro Patas, assim como seus voluntários e colaboradores, utiliza a tecnologia e a internet como ferramentas essenciais para otimizar suas atividades de resgate, adoção e campanhas de conscientização. No entanto, a dinâmica da sociedade contemporânea, caracterizada pela mobilidade e pela ausência de fronteiras físicas claras, impõe a necessidade de um cuidado redobrado para evitar incidentes que possam comprometer a segurança dos dados e informações da organização.

Nesse contexto, a segurança da informação torna-se uma atividade fundamental para a proteção de todos os ativos tangíveis e intangíveis da Quatro Patas, como sua imagem, reputação, conhecimento, patrimônio e, principalmente, a própria informação. É crucial que todos os membros da organização, sejam eles parte da administração, voluntários ou colaboradores, pratiquem e disseminem práticas seguras no ambiente digital.

Em resposta a essas demandas, está sendo implementado o Sistema de Gestão de Segurança da Informação (SGSI) da Quatro Patas, cuja diretriz principal é a Política de Segurança da Informação (PSI). Este documento foi elaborado para atender às especificidades do segmento de proteção animal e garantir a integridade, confidencialidade e disponibilidade das informações tratadas pela Quatro Patas.

Para que a Quatro Patas alcance o objetivo de proteger seus ativos durante a execução de suas atividades de resgate e proteção aos cães, é imperativo que todos sigam as novas regras estabelecidas. A adesão às políticas de segurança da informação é vital para a continuidade e o sucesso das operações da organização, assegurando a proteção de dados sensíveis e a manutenção da confiança da comunidade.

2 OBJETIVOS

A Política de Segurança da Informação (PSI) da Quatro Patas é aplicável a todos os aspectos operacionais, administrativos e tecnológicos da organização. Seus objetivos principais são:

- Estabelecer Diretrizes Estratégicas e Princípios de Proteção: Definir diretrizes estratégicas e princípios para proteger os ativos tangíveis e intangíveis da Quatro Patas, incluindo imagem, reputação, propriedade intelectual, bancos de dados, conhecimentos adquiridos e recursos de tecnologia da informação e comunicação (TIC), além das informações sensíveis dos animais resgatados e dos colaboradores.

- Orientar a Tomada de Decisões e Atividades Operacionais: Guiar a tomada de decisões e a execução das atividades de todos os colaboradores, voluntários e parceiros da Quatro Patas, tanto em ambientes físicos quanto digitais, em conformidade com as normas internas e a legislação vigente.

- Promover Atividades Seguras: Estabelecer princípios que assegurem a realização de atividades de resgate, proteção e adoção de maneira segura, evitando danos à reputação da Quatro Patas e garantindo a proteção dos dados envolvidos nesses processos.

- Construir uma Cultura de Segurança da Informação: Fomentar uma cultura de uso seguro e responsável das informações, capacitando todos os envolvidos a agir com segurança e responsabilidade no ambiente digital.

- Preservar a Confidencialidade, Integridade e Disponibilidade das Informações: Garantir a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e dos recursos de TIC da Quatro Patas, protegendo-os contra acessos não autorizados, alterações indevidas e outros riscos.

- Definir Normas e Procedimentos de Segurança da Informação: Orientar a criação de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos necessários para assegurar a conformidade com a PSI e a proteção eficaz dos ativos da organização.

A Quatro Patas está comprometida em seguir estas diretrizes para assegurar que todos os dados e informações sob sua responsabilidade sejam manejados de forma segura e ética, contribuindo para o bem-estar dos animais e a confiança da comunidade.

3 ABRANGÊNCIA

Esta PSI é um normativo interno, aplicável a todos os colaboradores que venham a ter acesso e/ou utilizem informações, recursos TIC e demais ativos intangíveis da ONG4P. Este normativo tem valor jurídico e aplicabilidade imediata.

4 DIRETRIZES GERAIS

4.1 Interpretação

4.1.1 Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da ONG4P.

4.1.1.1 Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da ONG4P e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

4.2 Propriedade

4.2.1 As informações geradas, acessadas, recebidas, manuseadas e armazenadas, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis da ONG4P e mantidas, são de propriedade e de direito de uso exclusivos da unidade.

4.2.2 Os recursos de TIC fornecidos pela ONG4P e mantidas, para o desenvolvimento de atividades estudantis, acadêmicas e profissionais, são de propriedade da unidade ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e, por isso, devem ser utilizados apenas para o cumprimento da finalidade a que se propõem.

4.2.3 Todos os ativos tangíveis e intangíveis da ONG4P e mantidas só podem ser utilizados para o cumprimento das atividades profissionais e educacionais, limitados à função do profissional responsável.

4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da ONG4P e mantidas, atuais e futuros, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais, quando prévia e expressamente autorizada.

4.2.5 Todos os profissionais poderão fazer menção da marca em conteúdos e materiais, para citação do local onde trabalha, mas, em hipótese alguma, poderá a marca ser utilizada para criação de perfis em mídias sociais em nome da instituição e/ou se fazendo passar por ela.

4.3 Classificação da informação

4.3.1 Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

4.3.1.1 Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à instituição e aos profissionais.

4.3.1.2 Informação interna: informação que pode ser divulgada para os cliente e profissionais da instituição, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

4.3.1.3 Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem

afetar a reputação e a imagem da instituição ou causar impactos graves, sob o aspecto financeiro, legal e normativo.

4.3.2 Rotulagem da informação: quando se tratar de informações não públicas, devem ser rotuladas no momento em que forem geradas, armazenadas e disponibilizadas.

4.3.2.1 Para informações geradas e/ou armazenadas em mídias removíveis ou papel, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.

4.3.2.2 Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados e Plano Diretor de Segurança, Políticas de Uso.

4.3.3 Em respeito à classificação da informação, todos os clientes e profissionais devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.

4.3.3.1 Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à instituição, incluindo a internet e mídias sociais, sem prévia e expressa autorização da ONG4P e/ou mantidas.

4.3.4 Todos profissionais devem respeitar o sigilo profissional e contratual. Por isso, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, fornecedores, prestadores de serviços ou demais detalhes institucionais críticos.

4.3.5 A GTI é responsável por homologar os mecanismos de criptografia, cifragem ou codificação para o armazenamento e a transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade.

4.4 Integridade de equipamentos

4.4.1 Os ativos críticos para a instituição devem estar protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar a sua contínua integridade e disponibilidade.]

4.5 Internet

4.5.1 Os recursos de conectividade são fornecidos para atender ao propósito administrativo e profissional, visto que o acesso à internet é um direito essencial para o exercício da cidadania no Brasil. No entanto, os colaboradores devem fazer uso da internet em estrita observância das leis em vigor, respondendo pelo seu descumprimento.

4.5.2 O acesso à internet é concedido aos profissionais por meio da identidade digital (login e senha) intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

4.6 Correio eletrônico

4.6.1 A utilização do correio eletrônico corporativo deve se ater à execução das atividades profissionais, respeitando as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

4.6.2 O correio eletrônico corporativo pode ser utilizado no dispositivo móvel particular, porém o acesso às mensagens e às informações institucionais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, visto que pode ocorrer por ato de liberalidade e/ou conveniência sem a expressa e prévia requisição da instituição.

4.6.3 A utilização de correio eletrônico particular ou público é permitida apenas para a transmissão ou recebimento de conteúdo ou informações particulares, e desde que não lhe seja dada prioridade sobre as atividades profissionais, não provoque efeitos negativos para qualquer outro usuário, não viole ou prejudique a rede corporativa e não viole norma vigente da ONG4P e mantidas.

4.6.3.1 O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da ONG4P e mantidas.

4.7 Rede sem fio (Wi-Fi)

4.7.1 A ONG4P, quando possível, oferece à seus funcionários, nos ambientes autorizados, uma rede sem fio (Wi-Fi) própria para finalidades profissionais e administrativas.

4.7.2 Somente colaboradores expressamente autorizados podem ter acesso à rede sem fio (Wi-Fi) da instituição e devem comprometer-se a fazer uso seguro desse recurso.

4.7.2.1 Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização do gestor imediato.

4.8 Recursos de TIC institucionais

4.8.1 Os recursos de TIC da ONG4P são destinados a finalidades estritamente profissionais, reservadas às atividades e permissões designadas para os usuários.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da ONG4P.

4.8.3 Para a proteção das informações, os arquivos digitais contendo informações da ONG4P e mantidas devem ser armazenados nos servidores de arquivos destinados às áreas e setores específicos, com acesso restrito, considerando que ameaças externas, tais como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas podem afetar a segurança de tais informações.

4.8.3.1 Os colaboradores devem armazenar os arquivos digitais nos servidores de arquivos específicos e com acesso restrito, disponibilizados na rede corporativa.

4.8.3.2 A GTI e o CRC são responsáveis por realizar as cópias de segurança dos arquivos digitais (backup) armazenados nos servidores de arquivos específicos da ONG4P.

4.8.3.3 A ONG4P não se responsabiliza pelos arquivos digitais armazenados nas estações de trabalho, nos notebooks, tablets e smartphones disponibilizados pela instituição. Em casos de desligamento ou rescisão contratual, os arquivos digitais serão apagados.

4.8.4 Todos os recursos de TIC da ONG4P, incluindo os softwares, devem ser inventariados e identificados pela GTI.

4.8.5 Só é permitida a utilização de softwares e hardwares legítimos, previamente homologados ou autorizados pela GTI, sejam eles onerosos, gratuitos, livres ou licenciados.

4.8.6 O desenvolvimento, a manutenção ou definição de aquisição de aplicativos e de sistemas no mercado são de responsabilidade da GTI e do CRC, e precisam atender aos requisitos de segurança em todas as etapas dos processos, a fim de garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

4.8.7 Todas as modificações nos recursos de TIC da ONG4P, principalmente em sistemas e na infraestrutura tecnológica, devem ser realizadas e/ou autorizadas pela GTI ou pelo CRC, e de maneira controlada para identificar os possíveis riscos e prevenir impactos à instituição, além de garantir a disponibilidade dos recursos de TIC e a possibilidade de restauração do ambiente original em caso de incidentes não previstos.

4.8.8 A utilização de recursos deve ser monitorada pela GTI e pelo CRC, aos quais cabe realizar projeções constantes para que os recursos de TIC suportem necessidades tecnológicas futuras.

4.8.9 É vedado o uso de recurso de TIC da ONG4P para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com o propósito profissional e as diretrizes da ONG4P.

4.8.10 Todo recurso de TIC de propriedade da ONG4P, incluindo os dispositivos móveis, devem utilizar recursos de segurança, como senha de bloqueio automático, antivírus, antispyware, firewall e mecanismos de controle de softwares maliciosos.

4.8.11 A retirada de qualquer equipamento, bancos de dados ou software das instalações da ONG4P, ou da sua infraestrutura tecnológica, deve ser realizada pela GTI e pelo CRC, quando prévia e formalmente autorizada pelo gestor imediato ou por necessidade da GTI ou do CRC.

4.8.12 Dispositivos móveis institucionais

4.8.12.1 O uso de dispositivos móveis de propriedade da ONG4P não é permitido por terceiros e prestadores de serviços.

4.8.12.2 Os dispositivos móveis institucionais devem conter a menor quantidade possível de informações da ONG4P. Arquivos digitais com informações da ONG4P, devem ser armazenados em servidores específicos para esse fim.

4.8.12.3 Em casos de roubo, perda ou furto do dispositivo móvel institucional que contenha informações da ONG4P, o colaborador deve registrar o Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GTI.

4.9 Recursos de TIC particulares

4.9.1 É vedada a conexão dos recursos de TIC particulares na rede corporativa da ONG4P.

4.9.1.1 Os colaboradores são autorizados a utilizar os recursos de TIC particulares, conectados à rede institucional, exclusivamente para as suas funções no âmbito profissional, atendendo aos princípios desta Política.

4.9.1.2 A ONG4P não têm qualquer responsabilidade sobre a utilização dos softwares, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos colaboradores.

4.9.2 Os recursos de TIC particulares previamente autorizados a acessar os conteúdos e serviços fornecidos pela ONG4P devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança, como antivírus e firewall, a fim de mitigar os riscos de exposição da instituição a ameaças.

4.9.3 Todo recurso de TIC particular trazido para as dependências da ONG4P é de inteira responsabilidade de seu proprietário, incluindo os dados e softwares nele armazenados ou instalados.

4.9.4 A ONG4P não será responsabilizada por qualquer perda, furto ou avaria dos recursos de TIC particulares.

4.9.5 Dispositivos móveis particulares

4.9.5.1 O uso de dispositivos móveis particulares é permitido dentro do perímetro da ONG4P, desde que não interfira nas atividades profissionais e esteja de acordo com as leis em vigor.

4.9.5.2 Dentro do perímetro físico e lógico em que informações confidenciais são armazenadas ou processadas, a ONG4P deve restringir a entrada e circulação de dispositivos móveis particulares.

4.10 Armazenamento de informações

4.10.1 Todos devem manter as informações da ONG4P armazenadas no local apropriado e destinado a esse fim.

4.10.2 Os colaboradores devem armazenar as informações digitais da ONG4P nos servidores da rede corporativa que possuem controle de acesso e cópia de segurança. As informações físicas devem ser guardadas em gavetas, armários trancados ou local apropriado e seguro quando não estiverem sendo utilizadas.

4.10.3 A ONG4P devem solicitar o apagamento e/ou a remoção de conteúdos que estejam nos dispositivos móveis particulares, na internet, nas mídias sociais e/ou em aplicativos, sempre que os mesmos oferecerem riscos aos colaboradores e/ou à instituição, que forem contrários à legislação nacional vigente, que possam configurar algum tipo de dano à instituição.

4.11 Repositórios Digitais

4.11.1 Os repositórios digitais para o uso institucional são destinados ao armazenamento, à criação, ao compartilhamento e à transmissão de arquivos de informações da ONG 4 Patas ou de suas mantidas, desde que previamente autorizados, homologados e disponibilizados pela equipe de Tecnologia da Informação (TI).

4.11.2 A utilização dos repositórios digitais para o uso institucional deve estar de acordo com os requisitos de segurança descritos nesta Política.

4.11.3 É proibido o armazenamento de arquivos digitais pessoais nos repositórios digitais para uso institucional.

4.11.4 Em caso de desligamento do colaborador, ou término de contrato de prestação de serviços dos alunos, os arquivos mantidos nos repositórios digitais de uso institucional serão excluídos.

4.11.5 Nos repositórios digitais de uso institucional é proibida a criação, o armazenamento, o compartilhamento e a transmissão de arquivos de informações referentes a qualquer tipo de atividade ilegal.

4.12 Mídias Sociais

4.12.1 O uso das mídias sociais pela equipe da ONG 4 Patas deve ser alinhado com os valores e objetivos da organização.

4.12.2 É proibida a divulgação de informações confidenciais ou sensíveis da ONG sem autorização prévia da direção.

4.12.3 A interação nas mídias sociais deve ser realizada de forma respeitosa e ética, evitando qualquer forma de discriminação, bullying ou comportamento inadequado.

4.13 Mesa Limpa e Tela Limpa

4.13.1 Os colaboradores devem manter suas mesas e telas de trabalho limpas e organizadas para garantir a segurança das informações e a eficiência no trabalho.

4.13.2 É importante proteger informações confidenciais de olhares não autorizados, mantendo as telas dos computadores bloqueadas quando não estiverem em uso.

4.14 Áudio, Vídeos e Fotos

4.14.1 A captura e o armazenamento de áudio, vídeos e fotos devem ser feitos com autorização prévia das partes envolvidas, especialmente no caso de animais resgatados ou colaboradores da ONG.

4.12.2 O uso dessas mídias deve estar em conformidade com as políticas de privacidade da ONG e as leis de proteção de dados vigentes.

4.15 Uso de Imagem, Som da Voz e Nome

4.15.1 A utilização da imagem, som da voz e nome de colaboradores ou beneficiários da ONG 4 Patas em materiais de divulgação deve ser feita mediante consentimento prévio e por escrito.

4.15.2 É importante respeitar a privacidade e os direitos das pessoas ao utilizar suas imagens ou informações pessoais em qualquer tipo de mídia.

4.16 Aplicativos de Comunicação

4.16.1 O uso de aplicativos de comunicação para assuntos institucionais deve ser realizado apenas através de ferramentas autorizadas pela ONG.

4.16.2 É proibido o compartilhamento de informações confidenciais ou sensíveis através de aplicativos de comunicação não autorizados.

4.17 Monitoramento

4.17.1 A ONG 4 Patas reserva-se o direito de monitorar o uso de sistemas de informação e comunicação para garantir a conformidade com esta política e proteger a segurança das informações.

4.17.2 O monitoramento será realizado de forma ética e em conformidade com as leis de privacidade e proteção de dados aplicáveis.

4.18 Combate à Intimidação Sistemática (Bullying)

4.18.1 A ONG 4 Patas está comprometida em combater qualquer forma de intimidação sistemática, incluindo o bullying online ou offline.

4.18.2 Os colaboradores são encorajados a relatar qualquer incidente de bullying ou comportamento inadequado à equipe de recursos humanos ou à direção da ONG.

4.19 Contratos de Trabalho e de Prestação de Serviços

4.19.1 Os contratos de trabalho e de prestação de serviços devem incluir cláusulas de confidencialidade e proteção de informações para garantir a segurança dos dados da ONG.

4.19.2 É responsabilidade dos colaboradores e contratados respeitar as políticas de segurança da informação da ONG durante e após o término do contrato.

4.20 Segurança da Informação

4.20.1 Todos os colaboradores da ONG 4 Patas devem estar cientes das políticas e procedimentos de segurança da informação e seguir as diretrizes estabelecidas para proteger os dados da organização.

4.20.2 É fundamental proteger a confidencialidade, integridade e disponibilidade das informações da ONG, adotando medidas de segurança adequadas e reportando qualquer incidente de segurança à equipe de TI.

Esta política de informação foi desenvolvida para promover o uso responsável e seguro das tecnologias e mídias pela equipe da ONG 4 Patas, garantindo a proteção das informações confidenciais e a integridade dos dados da organização.

5 PAPEIS E RESPONSABILIDADES

5.1 Todos

5.1.1 Ter conhecimento e ser capaz de transmitir e aplicar de forma clara os Princípios de Segurança da Informação.

5.1.2 Proteger os ativos tangíveis e intangíveis de propriedade ou sobre responsabilidade da ONG4P contra todos e qualquer tipo de ameaça, como acesso, compartilhamento ou modificações, não autorizadas, de conteúdos e informações.

5.1.3 Preservar e proteger os recursos institucionais, a marca, a reputação, a propriedade intelectual, informações e conteúdos, internos ou provenientes de terceiros, que estejam sob responsabilidade da instituição ONG4P.

5.1.4 Zelar pelo patrimônio, utilizando os recursos físicos e lógicos fornecidos com responsabilidade.

5.1.5 Evitar a exposição não autorizada de informações, projetos ou dados internos sobre pacientes, visando laudos e recursos laboratoriais e informações sensíveis da instituição e colaboradores terceiros em sigilo.

5.1.6 Prevenir e reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

5.1.7 Manter-se informado sobre mudanças nas políticas, normas de segurança da informação e diretrizes internas da ONG4P.

5.1.8 Reportar os incidentes que possam impactar na segurança das informações da ONG4P, imediatamente, por meio do endereço seguranca@ongquatropatas.br.

5.2 Gestores

5.2.1 Instruir os colaboradores de sua equipe e terceiros sobre as responsabilidades e uso seguro dos ativos tangíveis e intangíveis da ONG4P, incentivando-os, inclusive, a realizar a disseminação deste conhecimentos e valores para demais membros da instituição e relacionados.

5.2.2 Responsabilizar-se pelas consequências dos usos e atividades delegados aos colaboradores que se encontram sob sua responsabilidade direta ou indireta.

5.2.3 Assegurar o cumprimento desta Política e das demais regulações por parte dos colaboradores supervisionados.

5.2.4 Contribuir ativamente para a investigação de incidentes de segurança da informação, ativos e colaboradores sob sua responsabilidade.

5.2.5 Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

5.2.6 Monitorar e classificar os usos e acessos a informações sensíveis, sob sua responsabilidade direta ou indireta, por parte de colaboradores e relacionados.

5.3 Colaboradores

5.3.1 Evitar exposição desnecessária em meios de comunicação pública, tais como redes sociais, das rotinas e procedimentos realizados dentro ou relacionados às atividades da ONG4P, preservando o sigilo de informações sensíveis e anonimato de terceiros envolvidos e pacientes, salvo casos autorizados precisamente por superiores responsáveis.

5.3.2 Não transportar, compartilhar ou mover informações internas da ONG4P e parceiros para fora das dependências da instituição, salvo casos previamente autorizados pelos superiores responsáveis.

5.3.3 Não compartilhar informações internas da instituição de modo informal ou por meios não oficiais da ONG4P.

6 DISPOSIÇÕES FINAIS

Este documento deve ser lido e interpretado segundo as leis brasileiras vigentes, no idioma postuguês, respeitando também as normas e procedimentos previstos pela ONG4P.

Quaisquer desvios das normas descritas neste documento serão consideradas violações e estarão sujeitas a sanções cabíveis ao caso segundo previsto pelo Regimento Geral, contratos de

prestação de serviços, contratos de trabalho, acordos oficializados com terceiros e nas demais normas da instituição.

Esclarecimentos sobre os conteúdos contidos nesta PSI ou demais procedimentos de segurança da informação adotados podem ser encaminhados para o endereço eletrônico seguranca@ongquatropatas.br.

Em caso de incidente, infração ou suspeita dessas ocorrências deve-se comunicar, de forma imediata,endereço eletrônico seguranca@ongquatropatas.br.

7 DOCUMENTOS DE REFERÊNCIA

7.1 APÊNDICE A – Procedimentos

7.1.1 Acesso ao servidor FTP

Para acessar o servidor FTP da ONG 4 Patas (ONG4P) o usuário deve possuir algum Cliente FTP como o Filezilla, onde as credenciais deverão ser usadas para acessar o servidor. Atualmente o servidor está no nome do usuário aluno e será por ele que a conexão será feita, caso haja a necessidade da criação de um novo grupo/usuário no servidor entrar em contato com a equipe de técnica da ONG4P.

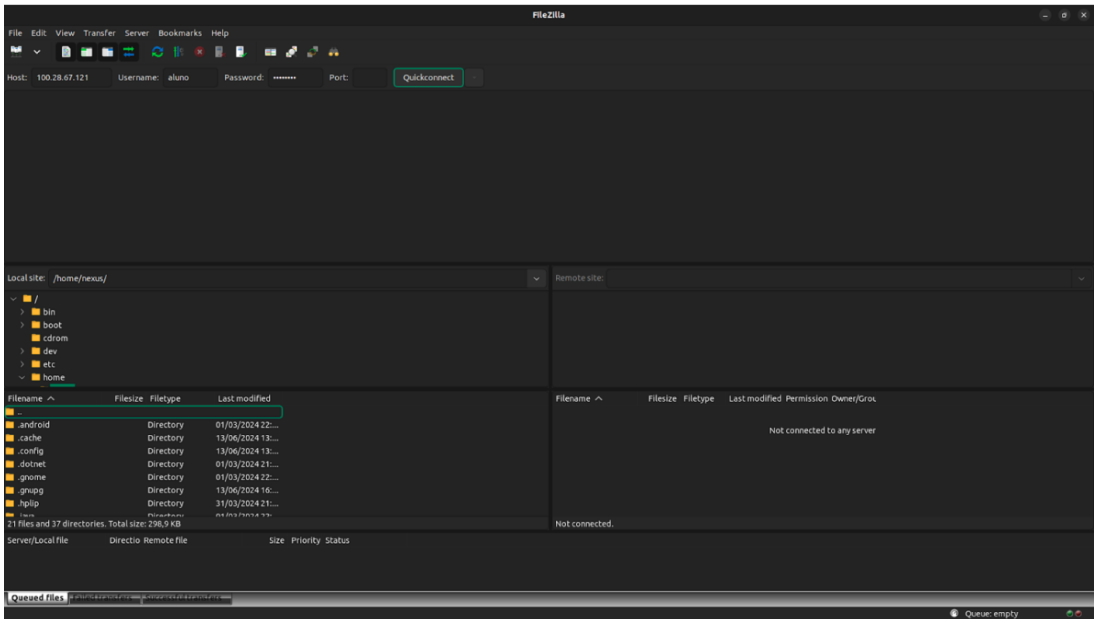
Acessar o servidor através de um cliente FTP

Esse tutorial será feito usando o Cliente FTP Filezilla caso haja a necessidade de baixá-lo acessar: https://filezilla-project.org/download.php?type=client.

Tendo o cliente instalado coloque as seguintes credenciais de acesso para se conectar ao servidor:

- Host: 100.28.67.121
- Username: aluno
- Password: aluno123

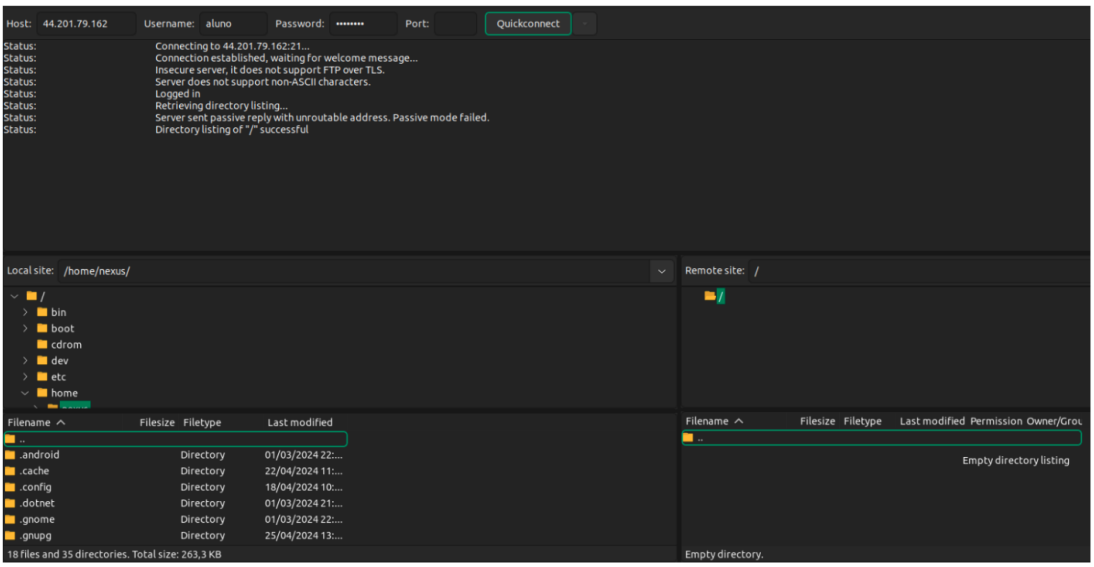
E clique em “Quickconnect”:

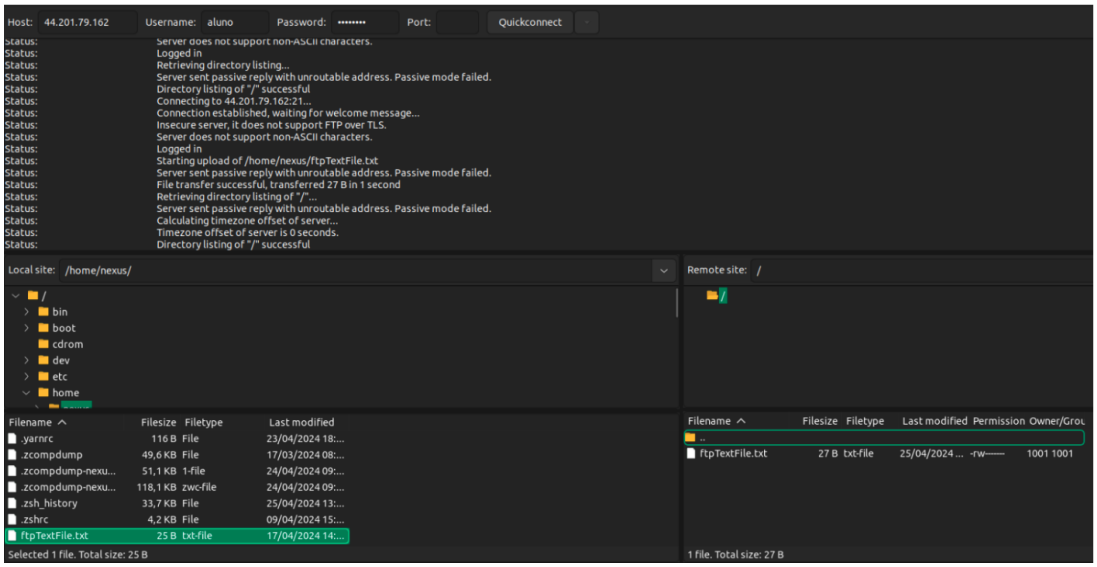


Após a conexão ser feita a transferência de arquivos pode ser feita. Cada Cliente FTP possui uma maneira de fazer a transferência de arquivos locais para o servidor e vice-versa. A maneira de fazer essa operação pelo Filezilla é a seguinte:

- O lado esquerdo representa os arquivos locais do computador, para enviá-los ao servidor clique duas vezes no mesmo e sua transferência será iniciada.

- O lado direito representa os arquivos do servidor, para enviá-los a máquina local clique duas vezes no mesmo e sua transferência será iniciada.





Para finalizar a conexão com o servidor clique no botão “Disconnect” na barra superior.

7.1.2 Acesso ao servidor HTTP

A aplicação da ONG 4 Patas (ONG4P) está localizada em uma Máquina Virtual (VM) que por sua vez está rodando na AWS EC2, o tutorial a seguir irá guiar o usuário a com acessar o código fonte da aplicação assim como rodá-lo.

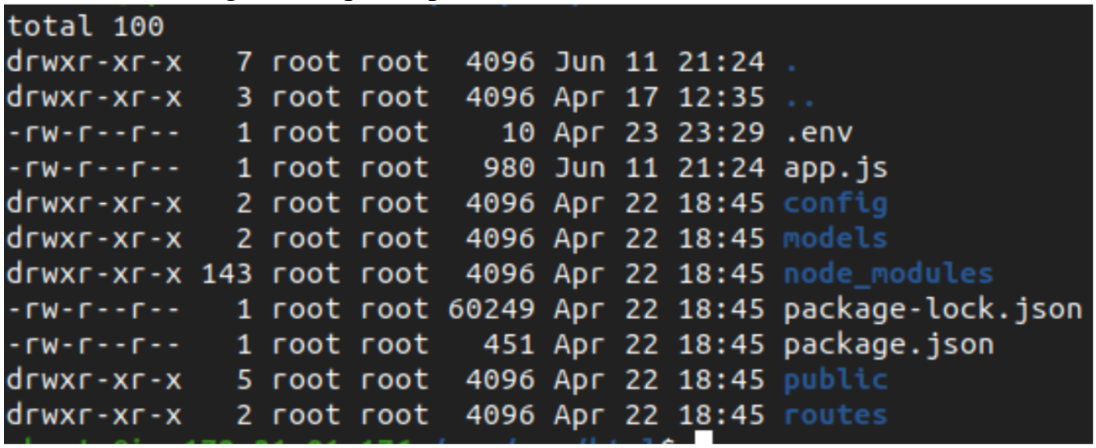
Acessar a VM do servidor HTTP Para que a conexão seja feita o usuário necessitará primeiramente da chave de acesso (.pem) da VM, que pode ser adquirida entrando em contato com a equipe técnica da ONG4P.

Tendo acesso a chave, a conexão poderá ser feita através do protocolo SSH da seguinte forma:

ssh -i "/<caminho_para_a_chave_de_acesso>/ong_quatro_patas_web_ftp_server.pem"ubuntu 100-28-67-121.compute-1.amazonaws.com

Caso haja algum erro de conexão o motivo pode ser que a VM está offline, para certificar entre em contato com a equipe técnica da ONG4P.

Após ter realizado a conexão navegue até a pasta com o código fonte da aplicação: **/var/www/html**, lá os seguinte arquivos podem ser encontrados:



Esses arquivos correspondem ao código fonte da aplicação.

Rodar a aplicação

Para que a aplicação possa ser iniciada é necessário que o banco de dados esteja online, caso não esteja entre em contato com a equipe técnica da ONG4P.

O banco de dados online a aplicação pode ser iniciada através do script:

- node app.js

Caso ocorra algum erro de permissão ao rodar um script nodejs o caminho fonte do deve ser especificado no comando:

- /home/ubuntu/.nvm/versions/node/v16.20.2/bin/node app.js

Com isso a aplicação será iniciada na porta 3000.

7.1.3 Acesso ao servidor DHCP

Acesso via SSH Obtenção do Endereço IP do Servidor DHCP: Para se conectar ao servidor DHCP é necessário que a máquina virtual que hospeda o mesmo esteja online, caso não esteja entre em contato com a equipe técnica da ONG4P.

No terminal da máquina virtual Ubuntu, é executado o comando ifconfig para obter o endereço IP. Este comando exibe informações sobre todas as interfaces de rede configuradas na máquina.

- É anotado o endereço IP exibido na interface de rede conectada. Por exemplo, o endereço IP pode ser 192.168.18.76

Conexão SSH ao Servidor DHCP:

- Para se conectar ao servidor DHCP via SSH, é utilizado um cliente SSH apropriado. Para usuários do Windows, recomenda-se o uso do cliente PuTTY. Para usuários de Linux ou macOS, o terminal integrado pode ser utilizado.

No cliente SSH, inserir as seguintes informações de conexão:

- ssh username@192.168.18.76
  - Substituir username pelo nome de usuário correto da máquina virtual fornecido pela equipe técnica da ONG4P.
  - Substituir 192.168.18.76 pelo endereço IP do servidor DHCP obtido anteriormente fornecido pela equipe técnica da ONG4P.
- Após a execução do comando, será solicitado a inserção da senha do usuário da máquina virtual. Inserir a senha corretamente para estabelecer a conexão.

8 GLOSSÁRIO

CRC: Centro de Recursos Computacionais.
FIREWALL: Sistema de segurança que monitora e controla o tráfego de rede.
GTI: Gestão de Tecnologia da Informação.
ONG4P: Refere-se à Organização Não Governamental Quatro Patas.
PSI: Política de Segurança da Informação.
SGSI: Sistema de Gestão de Segurança da Informação.
TIC: Tecnologia da Informação e Comunicação.