(AP-POL003)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Área Emissora (Owner)	Compliance
Aplicação	Todas as áreas
Nível de confidencialidade	Interna - Externa
Periodicidade de revisão	Anual
Autor	Karina Gregorio
Revisores	Edmar Primio
Aprovadores	Luiz Gênova - CEO

Palavras chaves	Autenticidade, Legalidade, Segurança, Confidencialidade, Disponibilidade, Integridade, Informação,
Código de referência	(AP-POL003)

Políticas relacionadas	AP-POL002 – Política de Privacidade de dados, AP-POL004 – Política de Instalação Software e Hardware – AP-POL005 – Política Geral de Tecnologia da Informação – AP-POL006 – Política de Segurança Cibernética – AP-POL008 – Política de Mesa e Tela Limpa – AP-POL009 – Procedimentos de conscientização de segurança da informação – AP-POL010 – Política de gestão de incidentes
Data da Aprovação e entrada e vigor	07/05/2026
Data do vencimento	07/05/2027

1. OBJETIVOS

A Política de Segurança da Informação, também referida como “PSI”, é o documento que define e orienta as regras corporativas da Amigoo Pet Serviços de Assistência para Animais Domésticos Ltda, doravante designado “**APET**”.

Esta Política de Segurança da Informação (PSI) está fundamentada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da Segurança da Informação, bem como está em consonância com as leis vigentes em nosso país a Lei Geral de Proteção de Dados Pessoais 13.709 (LGPD) e o Decreto Lei 9.637 que institui a Política Nacional de Segurança da Informação. Esta Política de Segurança da Informação (PSI) tem por objetivo:

Estabelecer diretrizes e normas que permitam aos colaboradores em geral da **APET** seguir padrões de comportamento, relativo à Segurança da Informação, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Conduzir a definição de procedimentos específicos de Segurança da Informação, bem como a implementação de controles e processos.

Preservar as informações da **APET** e dos pilares da Política de Segurança da Informação quanto a:

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Legalidade

2. DISPOSIÇÕES GERAIS

2.1 Termos e Definições

Ativo: Bens da empresa que tem valor econômico, incluída a informação e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Autenticidade: Consiste em assegurar que a pessoa, fonte e/ou dados, não foram alterados ou modificados por terceiros e que são completamente confiáveis.

Colaborador interno: Qualquer pessoa que execute alguma atividade com fins profissionais e que possua algum tipo de contrato com a empresa (Colaborador, e estagiários, por exemplo).

Colaborador Externo: Qualquer pessoa contratada por empresa terceirizada e que execute alguma atividade com fins profissionais nas dependências da **APET**, sem vínculo empregatício (Por exemplo, consultores e prestadores de serviços).

Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Informação: Todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Integridade: Capacidade de garantir que a informação está mantida em seu estado original, conforme foi concebida, possuindo conduta reta, ética, justa e honesta visando protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão;

Legalidade: Determina que devemos seguir e estar em conformidade com as Leis, Políticas, Procedimentos vigentes.

Parceiros: Qualquer colaborador contratado por terceiros que tenha ligação com o serviço prestado pela **APET** e suas informações e que não tenha nenhum vínculo empregatício ou mesmo contrato de prestação de serviços direto com a **APET** (Ex. Assistência 24h, distribuidores).

Segurança da Informação: Preservação da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação.

SPAM: E-mails não solicitados, normalmente enviados para muitas pessoas, que, geralmente, oferece, pede ou informa algo sem ser solicitado permissão.

Usuário: Todo colaborador interno ou externo, que contribui para a execução de atividades dentro da companhia, seja ele, funcionário, estagiário, aprendiz, consultor, ou prestador de serviços (terceirizado) e que tenha acesso aos recursos tecnológicos disponibilizados pela **APET.**

Vírus: Programa malicioso ou código malicioso que se propaga infectando a máquina de um usuário, alterando a forma de como o computador funciona e pode se propagar de um computador para o outro.

OneDrive: Serviço de armazenamento de arquivos em nuvem, com finalidade de armazenar arquivos de cada usuário.

Sharepoint: Serviço de armazenamento de arquivos em nuvem com backup e versionamento automático, para a finalidade de armazenar arquivos comuns à um grupo de usuários, departamento, ou ainda, à toda empresa.

3. APLICAÇÃO E ABRANGÊNCIA

As diretrizes estabelecidas nesta PSI deverão ser aplicadas em toda empresa, considerando o escritório central, bem como qualquer local onde se encontre ativos de informação da **APET** e devem ser seguidas por todos os colaboradores internos, externos e parceiros, devendo ser aplicada à informação em qualquer meio ou suporte.

4. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores, sejam internos ou externos, como resultado da atividade profissional contratada pela **APET**, pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

A informação da **APET**, produzida ou recebida deverá ser utilizada com senso de responsabilidade e de modo ético, integro e seguro, em benefício exclusivo dos negócios corporativos.

Todos os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados pelos colaboradores internos e externos para a realização das atividades exclusivamente profissionais.

A APET possui o direito de monitorar e registrar todo o uso das informações, sistemas e serviços. Para tanto, caso a **APET** considerar importante, poderão ser criados e implantados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgar necessário para reduzir os riscos, como, por exemplo, nos computadores de mesa, notebooks, nos acessos a Internet, no correio eletrônico e nos sistemas comerciais e financeiros, utilizados pela **APET** ou por terceiros.

5. REQUISITOS DA PSI

A PSI deverá ser comunicada a todos os colaboradores internos e externos da **APET**, visando garantir que todas as pessoas tenham conhecimento, estejam de acordo e pratiquem na empresa.

No caso de parceiros, deverá ser comunicada sempre que a parceria envolver acesso aos recursos tecnológicos da **APET.**

O uso do recurso do e-mail só é permitido para colaboradores internos, e para a central de atendimento – SAC que utiliza como endereço padrão atendimento@apetsaude.com.br., sendo proibida a criação de contas para demais terceiros que tenham ou não serviços vinculados a **APET**.

A PSI será revisada e atualizada periodicamente, no mínimo a cada ano, ou sempre que algum fato relevante ou evento ocorrer que motive a revisão antecipada dela conforme análise de Compliance e decisão dos Responsáveis da **APET.**

Deverá constar em todos os contratos da **APET**, o anexo de Acordo de Confidencialidade, ou cláusula de confidencialidade, como condição imprescindível para que possa ser concedido os acessos aos ativos de informações disponibilizados pela **APET.**

Deverá ser assinado previamente Acordo de Confidencialidade pelos prestadores de serviços e parceiros que recebem informações de projetos para fins de elaboração de orçamento, negociação, propostas, entre outros, que sejam consideradas como relevantes para o negócio da **APET**.

Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, de forma a minimizar possíveis riscos.

Todos os incidentes que afetam a Segurança da Informação devem ser reportados ao Compliance e Suporte de TI.

Um plano de contingência e continuidade do negócio deverá ser implementado e testado, no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação.

O desenvolvimento de projetos ou sistemas deverão obrigatoriamente seguir os requisitos de Segurança da Informação, incluindo a necessidade de planos de contingência e devem ser identificados na fase de levantamento de escopo de um projeto ou sistema. Estes requisitos devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Os ambientes de produção devem ser segregados e rigidamente controlados garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

Os ativos críticos ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados e ter o acesso controlado, registrado e monitorado. O ambiente deve ser dotado de garantia de energia elétrica e climatização.

Todo ativo de informação deve ser protegido de divulgação, modificação, furto ou roubo, através da aplicação de controles adequados à sua classificação.

O Compliance da **APET** estabelecerá e comunicará normas e responsabilidades específicas pela gestão e custódia dos ativos de informação sensíveis.

Qualquer alteração realizada em processos, procedimentos e tecnologias devem ser formalmente avaliadas considerando o atendimento aos requisitos desta PSI.

O Compliance estabelecerá procedimentos e responsabilidades específicas para o uso e gerenciamento dos ativos de informação disponibilizados pela **APET** quando estiverem fora das instalações da empresa.

A área de Suporte de TI será responsável por emitir todos os logins e acessos de softwares que estão dentro do escopo do suporte, como email, teams e permissão a arquivos da rede, utilizados na **APET**. Esta área deve buscar a convergência destes documentos para uma identidade única criando uma base de dados sob sua responsabilidade para consulta e identificação por todos os sistemas de controle de acesso físico e lógico da **APET.**

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta norma o responsável e/ou solicitante deverá documentá-las imediatamente ao departamento de Compliance e a área de Suporte de TI, para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

A **APET** exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, concedendo o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, adotar as medidas legais cabíveis e punir os infratores.

6. DAS RESPONSABILIDADES ESPECÍFICAS

6.1 Colaboradores em Geral

É de inteira responsabilidade de cada colaborador interno, externo ou parceiro, qualquer prejuízo ou dano que vier a sofrer ou causar a **APET** e/ou a terceiros, em consequência de não obediência às diretrizes e normas aqui referidas.

Cabe a todos os colaboradores da **APET**:

- Cumprir rigorosamente políticas, normas e procedimentos de segurança da informação estabelecidos neste documento;
- No caso de colaborador interno, buscar orientação do Compliance, quando houver dúvidas relacionadas à segurança da informação;
- No caso de colaborador externo e parceiros, deverá buscar orientação do seu departamento de Compliance e/ou seu superior sendo da mesma empresa prestadora de serviços, quando houver dúvidas relacionadas à segurança da informação.
- Proteger as informações contra o acesso, modificação divulgação ou destruição não autorizada pela **APET**;
- Assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse da **APET**;
- Comunicar imediatamente o Departamento de Compliance e a área de Suporte de TI, quanto a qualquer descumprimento ou violação desta política e/ou de suas Normas e Procedimentos, para que possam ser tomadas as medidas cabíveis e/ou traçar plano de ação para mitigação de riscos.

6.2 Diretorias, Gerências e Coordenações

Cabe as Diretorias, Gerências e Coordenações:

- Revisão e aprovação final da PSI.

- Ter comportamento exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores internos sob a sua gestão.
- Cumprir e fazer cumprir esta política, as normas e procedimentos de Segurança da Informação;
- Garantir que suas equipes participem dos treinamentos, possuam acesso e conheçam esta política, bem como das normas e procedimentos aqui estabelecidos;
- Requisitar a assinatura do Acordo de Confidencialidade, antes de conceder acesso às informações da empresa, para colaboradores externos que sejam eventuais, parceiros e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais;
- Identificar e solicitar previamente permissão de acesso, elencando os ativos de informação para prestadores de serviços em geral;
- Conciliar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;
- Comunicar imediatamente ao Departamento de Compliance e a área de Suporte de TI, referentes a eventuais violações da segurança da informação.

6.3 Da área de Suporte de Tecnologia da Informação

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores em geral com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

- Testar a efetividade dos controles utilizados e informar aos gestores os riscos residuais.
- Definir o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- O acesso à arquivos e dados de outros usuários por administradores e operadores dos sistemas computacionais será permitido somente mediante necessidade, como por exemplo, em casos de backup, manutenção, auditoria, testes no ambiente e grave suspeita de ato ilícito, que por sua vez deve ser justificado e documentado por pessoa autorizada.

- Segregar as funções administrativas e operacionais de forma a restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos minimizar, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança em especial para sistemas com acesso público fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Criar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a **APET**.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por TI.
- Quando ocorrer movimentação interna dos ativos de TI (equipamentos/,software e etc.), garantir que as informações de um usuário serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão, necessárias para garantir a segurança requerida pelas áreas de negócio.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e a qualquer outro ativo de informação a um responsável identificável como pessoa física.
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso.
- Garantir que todos os novos ativos da informação da empresa só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual no caso de uso de terceiros para controle e responsabilização.
- Definir as regras formais para instalação de Software e Hardware em ambiente de produção corporativo.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.

- É responsável pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir da forma mais rápida possível o bloqueio de acesso de usuários, a partir de solicitação formal, por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
    - Uso da capacidade instalada da rede e dos equipamentos;
    - Tempo de resposta no acesso à Internet e aos sistemas críticos da **APET**;
    - Períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da **APET**;
    - Incidentes de segurança (vírus, trojans, furtos, acesso indevidos, etc.);
    - Atividade de todos os colaboradores internos, externos e parceiros, durante os acessos às redes externas, inclusive Internet (ex.: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, etc.);
    - Garantir que todos os servidores, estações e demais dispositivos com acesso a rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Propor à diretoria da **APET**, as versões da PSI e as Normas de Segurança da Informação.
- Propor as metodologias e processos específicos para a Segurança da Informação, tais como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem a segurança dos ativos de informação da **APET**.

  Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pela Diretoria.
- Promover conscientização dos colaboradores internos, externos e parceiros em relação à relevância da Segurança da Informação para o negócio da **APET**, através de campanhas, palestras, treinamentos e outros meios.

- Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços.
- Programar configurações nas máquinas dos usuários da **APET** para garantir que em 3 (três) minutos sem utilização seja realizado automaticamente o bloqueio de tela do computador.
- Garantir que quaisquer documentos não confidenciais e confidenciais da APET, não sejam compartilhados com terceiros que não sejam reconhecidos via correio eletrônico, sem autorização prévia.

6.4 Departamento de Compliance e Gestão de Risco

- Garantir que **APET** esteja em conformidade com as Leis e Regulamentos vigentes.
- Responsável pela atualização periódica desta PSI.
- Realizar treinamentos periódicos de segurança da informação para os colaboradores da **APET.**
- Garantir que os colaboradores da **APET** estejam cientes e que estejam seguindo as regras, normas e condutas desta PSI.
- Certificar que os treinamentos de segurança da informação pela plataforma KnowBe4, estão sendo disponibilizados e que eles estão sendo realizados pelos colaboradores no prazo estipulado.
- Criará controles internos para identificar e gerenciar os riscos.
- Auxiliar os colaboradores quanto as dúvidas e questionamentos desta PSI.
- Criará o PCN de Segurança da Informação para minimizar os riscos para casos de vazamentos de dados pessoais.

7. DO MONITORAMENTO E AUDITORIA

Para garantir as regras mencionadas na PSI, a **APET** se reserva no direito de:

- Estabelecer procedimentos de monitoramento nas estações de trabalho, servidores, e-mail, conexões à Internet, dispositivos móveis ou wireless e outros componentes da

rede. A informação gerada por este monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

- Divulgar internamente, por determinação da Diretoria da **APET**, às pessoas autorizadas as informações obtidas pelo monitoramento e auditoria bem como tornar pública no caso de exigência judicial;
- Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta PSI;
- Aplicar procedimentos de proteção preventivos e detectivos para garantir a segurança das informações e dos perímetros de acesso às mesmas;
- Instalar as câmeras de vigilância se julgar necessárias.

8.TREINAMENTOS

A **APET** estabelece treinamentos obrigatórios de segurança da informação através da plataforma online Knowbe4 e através do departamento de Compliance com treinamentos presenciais para todos os colaboradores internos e externos. O link para acesso a plataforma é encaminhado via e-mail para todos os novos colaboradores, na qual, pode ser realizado o primeiro acesso.

Estes treinamentos visam:

- Garantir que os colaboradores possuam a conscientização das ameaças cibernéticas que existam como: phishing, engenharia social, malware entre outros. Além disto, compreenderem quais riscos cada um pode causar.
- Orientar quanto ao nível classificação da informação, para que, elas possam ser tratadas e protegidas conforme sua identificação se é confidencial, sensível, restritas, livres, entre outros tipos de classificação.
- A Redução de incidentes, visto que, serão abordados temas para conscientização sobre possíveis ataques e ameaças e isto orientará como agir e seguir nestes casos.
- Cumprimento de regulações e leis que exigem, que os colaboradores das organizações, tenham treinamentos de segurança da informação.

8.1 Módulos dos treinamentos – Knowbe4

Os novos colaboradores iniciam o primeiro módulo de treinamento com uma pesquisa introdutiva, sendo elas, a avaliação de conhecimento sobre conscientização em segurança (SAPA) e a pesquisa sobre cultura de segurança. Este módulo tem como objetivo identificar o nível de conhecimento de cada colaborador sobre o tema de segurança da informação.

O Segundo módulo reforçará sobre a conscientização de segurança da informação com os temas referentes a princípios básicos da navegação segura, comprometimento de e-mail corporativo, segurança de dispositivos móveis e ameaças internas acidentais.

Após a finalização dos dois primeiros módulos os seguintes serão atribuídos para o módulo que está em andamento que possuem vários outros temas como: Princípios básicos da navegação segura, segurança de dispositivos móveis, comprometimento de e-mail corporativo, ameaças internas acidentais entre outros.

8.2 Do prazo e validade dos treinamentos

Os treinamentos terão prazo estipulado para finalização, os quais serão mencionados no recebimento do e-mail e podem ser acessados no portal do knowbe4 em ‘ver detalhes’ do treinamento.

Enquanto os treinamentos estiverem em andamento, serão disparados e-mails lembretes reforçando a importância da realização e do prazo de vencimento.

8.3 Das Penalidades

A não realização dos treinamentos podem causar penalidades, visto que, eles foram implementados para conscientizar e minimizar os riscos cibernéticos que podem afetar a **APET.**

Se o treinamento não for realizado até 2 (dois) dias antes do vencimento, o seu gestor será notificado pelo departamento de Compliance para que ele esteja ciente e acompanhe o andamento do treinamento até que seja finalizado.

Após o vencimento dos treinamentos o departamento de Compliance juntamente com o gestor do colaborador poderá aplicar penalidades conforme descritas no item 17 desta PSI.

9. IDENTIFICAÇÃO E AUTENTICAÇÃO

- O acesso aos dados e informações da rede, sistemas informatizados e demais recursos tecnológicos disponibilizados pela **APET**, deve ser registrado, identificado e controlado;
- Todos os dispositivos utilizados para identificação dos colaboradores da **APET** tais como o número de matrícula, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais, deverão estar associados a uma pessoa física e atrelados de forma comprovada quanto aos seus documentos RG e/ou CPF.
- O registro de acesso tanto aos dados e informações da rede como aos sistemas informatizados, deve ser feito através de Logs.
- A identificação do acesso é feita através da conta do usuário (Login).
- Todo colaborador interno deve possuir uma conta de usuário e senha para os sistemas, desde que a função exercida na empresa exija atividades executadas com recursos de TI. No caso de colaborador externo, o mesmo deverá ser concedido apenas mediante autorização expressa do diretor ou coordenador responsável.
- A conta de usuário é única e intransferível.
- Todo e qualquer dispositivo de identificação pessoal, não poderá ser compartilhado com outras pessoas em nenhuma hipótese, sendo o colaborador ainda que externo, responsável pelo uso correto de suas informações de identificação, perante a **APET** perante a legislação (cível e criminal).
- A área de Suporte de TI deverá providenciar o registro e acesso de usuários à rede da empresa, somente mediante solicitação do RH ou Diretoria.
- As senhas devem ser criadas com expiração imediata, forçando a sua alteração pelo usuário no primeiro acesso.
- Os usuários deverão, sempre que possível, ter senha de tamanho variável, possuindo, no mínimo, 8 e no máximo 12 caracteres, alfanuméricos, utilizando caracteres especiais (@ # $ %) opcional e variação à caixa alta e caixa baixa (maiúsculo e minúsculo).
- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e guarda dos dispositivos de identificação que lhe forem designados.

- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).
- As senhas não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento.
- As senhas não devem ser constituídas de combinações óbvias de teclado, tais como “abcdefgh”, “87654321”, etc.
- Nos principais sistemas após 3 (três) tentativas de acesso, a conta do usuário deverá ser bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com área de Suporte de TI.
- Caso o colaborador interno esqueça sua senha, deverá requisitar formalmente a troca da mesma à área de Suporte de TI, responsável por cadastrar uma nova ou na impossibilidade de ambas deve solicitar ao seu superior direto.
- Caso o colaborador externo esqueça a sua senha, deverá solicitar para o seu superior da empresa prestadora de serviços, que solicitará nova senha formalmente através de seu representante ou contato estabelecido para os serviços previstos.
- Caso o usuário suspeite que terceiros obtiveram acesso indevido ao seu login/senha, deverá entrar em contato imediato com a área de Suporte de TI e solicitar alteração de sua senha.
- A área de Suporte de TI, determina que a periodicidade máxima, para troca das senhas é de 180 (cento e oitenta) dias, ou seja, 06 (seis) meses não podendo ser repetir as 3 (três) últimas senhas.
- Os sistemas forçaram as trocas de senhas dentro do prazos máximos definido no item anterior.
- Será estabelecido um lembrete para troca de senha, sempre que o prazo de 180 (cento e oitenta) dias estiver vencendo.
- Todos os acessos devem ser imediatamente bloqueados (inativados) quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o RH deverá imediatamente comunicar a área de Suporte de TI, a fim de que o acesso seja bloqueado imediatamente, e o login do usuário será mantido por no

mínimo 6 (seis) meses para fins de prevenção a fraude. Esta conduta também se aplica aos usuários cujo contrato ou prestação de serviços tenham se encerrado, bem como os usuários de testes e outras situações similares.

- O extravio, roubo ou perda da senha de acesso pelos usuários, deverá ser comunicado imediatamente a **APET**, a fim de que possam bloqueá-las e ser disponibilizado nova senha de acesso.
- Ficam aos Colaboradores internos e externos cientes de que, enquanto a **APET** não for cientificada dessa ocorrência, ficarão responsáveis pelos atos praticados por terceiros, através da utilização da senha, que provoquem danos aos servidores/ terceiros/demais usuários da **APET**.
- É de integral responsabilidade dos Colaboradores internos e externos, qualquer prejuízo ou dano que vierem a sofrer ou causarem a **APET** e ou a terceiros, em decorrência do uso inadequado ou indevido de sua senha, seja por conduta culposa ou dolosa.

10. DOS COMPUTADORES E RECURSOS TECNOLÓGICOS

- Os equipamentos utilizados por colaboradores internos, externos ou parceiros são de propriedade de cada indivíduo ou da **APET**, cabendo a cada um, para as atividades de interesse da empresa, a utilização correta e manuseio deles, bem como o cumprimento das recomendações constantes nos Procedimentos Operacionais de cada setor, que deverão ser previamente acordadas com a área de Suporte de TI.
- Os acessos, as informações da **APET**, são protegidos por áreas específicas para cada usuário, e são definidos pela diretoria, de acordo com função e responsabilidades.
- É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, realizados sem o conhecimento prévio e o acompanhamento de um técnico da área de Suporte de TI ou a quem este determinar. As áreas/núcleos que necessitarem realizar testes deverão solicitar previamente à área de Suporte de TI ficando responsável jurídica e tecnicamente pelas ações realizadas.

- Todas as atualizações e correções de segurança do sistema operacional da **APET** ou aplicativos deverão ser devidamente validados no respectivo ambiente de homologação, após a sua disponibilização pelo fabricante ou fornecedor.
- Os sistemas e computadores devem ter versões instaladas, ativadas e atualizadas permanentemente do software antivírus. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a TI imediatamente.
- Arquivos pessoais e/ou não pertinentes ao negócio da **APET** (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois estes podem sobrecarregar os servidores de arquivos em nuvem. Quando identificado a existência de arquivos pessoais, a área de Suporte de TI comunicará o responsável direto, determinando prazo para a remoção. Não tomada as devidas providências, a área de Suporte de TI poderá eliminar os arquivos diretamente do local onde se encontram.
- Documentos fundamentais para as atividades dos colaboradores da **APET** deverão ser salvos nas pastas sincronizadas do OneDrive ou Sharepoint, de acordo, com a propriedade do arquivo. Os arquivos gravados apenas localmente nos computadores (Ex. drive C:), não terão garantia de Backup e poderão ser perdidos caso ocorra uma falha no computador, furto ou qualquer sinistro, e assim acontecendo o usuário poderá ser responsável por negligência.
- A utilização de Modems (3G) somente será permitido conforme regra específica e ou de acordo com plano de contingência, mediante autorização dos gestores dos núcleos e de TI.
- A alteração de configuração dos equipamentos disponibilizados pela **APET**, só poderá ocorrer mediante autorização prévia e expressa da área de Suporte de TI.
- Deverão ser protegidos por senha (bloqueados), todos os terminais de computadores quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela **APET** devem ter imediatamente suas senhas padrões (default) alteradas.
- Acrescentamos que é explicitamente proibido a todos os colaboradores o uso de computadores e recursos tecnológicos da **APET** para as seguintes situações:

  - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem conhecimento e autorização do proprietário;
- Monitorar de forma discreta indivíduos por meio de dispositivos eletrônicos ou softwares, como por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores através de qualquer método;
- Utilizar qualquer tipo de meio tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Armazenar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- A utilização de recursos de terceiros em conjunto com recursos tecnológicos da **APET**. (Ex. Pendrive pessoal ou do cliente/parceiro, smartphones, palmtop, tablet, etc) sem a prévia autorização da TI;
- Utilizar software sem licença oficial do fabricante.

- As ferramentas devem ser utilizadas para fins e exercício de suas atividades, não sendo permitido a instalação de softwares, mesmo que seu perfil permita tal ação.

11. DO USO DE DISPOSITIVOS MÓVEIS

- Quando se descreve “Dispositivo Móvel” entende-se que qualquer equipamento eletrônico de propriedade da **APET**, ou aprovado e permitido pela área de Suporte de TI, com atribuições de mobilidade, tais como: notebooks, smartphones, pendrives, câmeras e outros.
- É permitido o uso de dispositivos móveis, desde que sejam de propriedade da **APET** e/ou homologados pela área de Suporte de TI.

- A **APET**, na qualidade de proprietária dos equipamentos fornecidos, se reserva ao direito de inspecioná-los, sempre que verificar necessário.
- Todos os colaboradores deveram realizar periodicamente cópia de segurança (backup) dos dados pertencentes à **APET** que estiverem de seu Dispositivo Móvel no OneDrive ou Sharepoint. Não será permitido backups de arquivos em pendrives.
- É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel, fornecido pela **APET**, notificar imediatamente ao seu Gestor Direto e a área de Suporte de TI. Este também deverá procurar a ajuda das autoridades policiais registrando, imediatamente, um boletim de ocorrência (BO).
- Todos os colaboradores devem estar cientes de que o uso indevido do Dispositivo Móvel, fornecido pela **APET**, caracterizará a aceitação de todos os riscos da sua má utilização, sendo este o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **APET** e/ou a terceiros.
- A disponibilização de notebook para o colaborador como ferramenta de trabalho para uso contínuo pressupõe a retirada do desktop e utilização de uma única máquina. O uso simultâneo de desktop e notebook deve ser autorizado pela Diretoria Executiva da **APET**, mediante análise prévia.

12. DO USO DE CORREIO ELETRÔNICO

- O uso do Correio Eletrônico da **APET** deve ser utilizado para fins corporativos e relacionados às atividades do colaborador dentro da empresa, não sendo permitido seu uso para fins pessoais, portanto por medidas de segurança e manutenção das políticas internas, a **APET** tem o direito de monitorar sempre que analisar necessário as caixas de e-mails de todos os colaboradores.
- Não é permitido aos colaboradores na utilização de uso do Correio Eletrônico da **APET**, sendo tratado como falta grave:
    - Enviar mensagens não solicitadas para múltiplos destinatários, (ex. correntes, casos interessantes, piadas), exceto se for relacionada a uso legítimo da empresa;

o Enviar qualquer mensagem através dos meios eletrônicos que torne seu remetente e/ou a **APET** ou suas empresas associadas vulneráveis a ações civis ou criminais;

o Divulgar informações confidenciais ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário deste ativo de informação;

o Falsificar informações de endereçamento, modificar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

o Deletar mensagens pertinentes de correio eletrônico quando qualquer uma das localidades da **APET** estiver sujeita a algum tipo de investigação;

o Produzir, transmitir ou divulgar mensagem que:

- ☐ Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **APET**;
- ☐ Contenha ameaças eletrônicas, tais como: spam, mail bombing, vírus de computador;
- ☐ Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- ☐ Inclua imagens criptografadas ou de qualquer forma mascaradas;
- ☐ Contenham anexo(s) superior(es) a: 25Mb para ENVIO (Interno e Internet) e 50Mb para RECEBIMENTO (Internet);
- ☐ Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- ☐ Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico e etc.;
- ☐ Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- ☐ Tenha fins políticos locais ou do país (propaganda política) e religiosos;
- ☐ Contenha material protegido por direitos autorais sem a permissão do detentor dos direitos.

- A **APET** poderá ainda tomar as medidas judiciais cabíveis para impedir o envio de mensagens com conteúdo ilegal ou spams por parte de seus Funcionários, Estagiários ou Colaboradores, o trânsito, armazenamento dessas mensagens em equipamentos pertencentes a **APET**, bem como o uso indevido de sua rede de computadores, sem prejuízo da propositura das ações judiciais para o ressarcimento pelas perdas e danos causados por referidos atos.
- A passividade por parte da **APET** em reprimir qualquer ação por parte de Funcionário, Estagiário ou Colaborador, não autorizada por esta política, não poderá ser interpretada como desistência por parte da **APET** de qualquer direito de fazê-lo no futuro.

13. DO USO DA INTERNET

- Os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet, podem ser analisados pela **APET** que, se necessário, pode bloquear qualquer arquivo, áudios, site, correio eletrônico, domínio ou aplicação armazenados na rede/Internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua PSI.
- Toda a Informação da Internet que é acessada, transmitida, recebida ou produzida está sujeita à auditoria e divulgação interna. Portanto, a **APET,** em total conformidade legal, reserva-se ao direito de monitorar e registrar todos os acessos à Internet.
- O uso da internet é permitido para fins profissionais, devendo o colaborador ficar atento aos sites que deseja acessar, para que sejam condizentes com suas ações. Casos de exceção serão previstos em documento próprio como regra de exceção para uso de internet (pode abranger sites de pesquisa, imposto de renda, bancos, receita federal, governamentais etc)
- Casos de exceção para o uso da internet e não previsto em documento específico deverá ser objeto de autorização pela área de Suporte de TI.
- Somente os colaboradores que estão devidamente autorizados a falar em nome da **APET** para os meios de comunicação poderão manifestar- se em nome da empresa, seja por e-mail, documento físico, entrevista online, podcast, entre outros.

- Somente os colaboradores que estão devidamente autorizados pela **APET** poderão copiar, captar imagens da tela, imprimir ou enviar para terceiros, devendo atender à Norma interna de comunicação e à norma interna de alçada, à Lei de Direitos Autorais, Proteção da Imagem garantida pela Constituição Federal e demais dispositivos legais.
- É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na Internet.
- Como regra geral, não poderá ser exposto, armazenado, distribuído, editado, impresso ou gravado através de qualquer recurso, material sexualmente explícito.
- Não é permitido acesso a sites de proxy.
- O acesso à internet é de uso exclusivo para colaboradores internos da **APET**, o compartilhamento com parceiros e clientes somente será efetivado com prévia autorização e homologação da área de Suporte de TI.
- São tratados como falta grave e estarão sujeitos a medidas disciplinares e/ou judiciais cabíveis os seguintes comportamentos, com ativos da **APET**:
    - Acesso a sites cujo conteúdo conflite com os valores e interesses da **APET**, estando o Funcionário, Estagiário ou Colaborador em horário de trabalho ou não;
    - Acessar, armazenar, divulgar e repassar qualquer material de conteúdo ilícito ou malicioso, como vírus, worms, cavalos de tróia ou programas de controle de outros computadores, bem como spams;
    - Efetuar upload ou distribuição de qualquer software, licenciado ou não a **APET**, ou dados de propriedade da **APET** ou de seus clientes;
    - Divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida;
    - Utilização de softwares de comunicação instantânea, tais como skype, Telegram, Facebook, Instagram, whatsApp, linkedin, e-mail pessoal, messenger e afins, exceto autorizados pela empresa;
    - Utilização de softwares de peer-to-peer (P2P), tais como utorrent e afins;

- Utilização de serviços de streaming, tais como Rádios On-Line e afins exceto em casos específicos e autorizados pela empresa.

14. DA INSTALAÇÃO DE SOFTWARES

- A instalação de softwares nos equipamentos da **APET** deverá ser feita pela área de Suporte de TI, devendo estes estarem devidamente licenciados.
- Existindo a necessidade de instalação de qualquer software por um colaborador da **APET**, deverá ser solicitado formalmente à área de Suporte de TI que fará uma pesquisa para a melhor alternativa levando em consideração, custo x benefício, devendo ainda o software ser de uso único e exclusivamente profissional.
- A reprodução não autorizada dos softwares instalados nos equipamentos fornecidos pela **APET** constitui uso indevido do equipamento e conforme estabelecido nesta política poderá gerar infração legal aos direitos autorais do fabricante.
- O download (baixar) de programas será permitido apenas mediante autorização do superior direto e da área de Suporte de TI, devendo este estar ligado diretamente às suas atividades na **APET** e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.
- Não é permitido efetuar upload (subida) de qualquer software licenciado a **APET** ou dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.
- O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos.
- Os colaboradores não poderão em hipótese alguma utilizar os recursos da **APET** para fazer o download ou distribuição de software ou dados pirateados, atividade está considerada delituosa de acordo com a legislação nacional.
- O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins.) não são permitidos.
- A área de Suporte de TI poderá fazer remotamente inventário de software, bem como verificação/monitoramento de softwares instalados, a fim de prevenir e eliminar uso

ilegal e problemas com direitos autorais, bem como monitorar a data de expiração das licenças já concedidas.

15. USO DE IMPRESSORAS

- O uso de impressoras da **APET** é para fins corporativos e relacionados às atividades do colaborador dentro da empresa, não sendo permitido, portanto, impressões de qualquer arquivo ou documento pessoal sem prévia autorização.
- As impressoras deverão ficar em locais apropriados e seguros.
- Será criado procedimento específico para uso de impressora, sendo que este deverá abordar: Impressões esquecidas na máquina, papéis em branco, erro de impressão, trava de papel, descarte correto de impressões entre outros.
- Todos os documentos impressos que possuírem dados sensíveis deverão ser armazenados em local seguro e que outros não tenham acesso.

16. DAS PENALIDADES

O não cumprimento desta Política e Norma a ela atreladas caberá:

- Na primeira infração, advertência verbal;
- Na segunda infração, advertência escrita com anotação de repetição de infração;
- Na terceira infração, suspensão não remunerada que pode durar até 30 (trinta) dias conforte art. 474 da CLT.
- Na quarta Infração, demissão por justa causa.

Com base no Artigo 482 da CLT um dos motivos que podem atrelar a demissão por justa causa ocorre devido ao não cumprimento de incontinência de conduta ou mau procedimento.

Nos casos em que a infração corresponder a atividades ilegais, ou ainda incorrer em dano à empresa ou a terceiros, serão encaminhados para a diretoria que poderá deliberar pela

demissão por justa causa, dispensando as advertências, não eximindo o infrator das medidas previstas pela legislação vigente, sendo que a **APET** cooperará ativamente com as autoridades nesses casos.

No caso de prestadores de serviços a ocorrência deverá ser levada até a diretoria que deliberará sobre a rescisão de contrato ou não do prestador.

Os Funcionários, Estagiários ou Colaboradores que infringirem as presentes condições de uso serão responsabilizados pelos danos e prejuízos de qualquer natureza que a **APET** venha a sofrer ou aqueles causados a terceiros.

17. DAS DISPOSIÇÕES FINAIS

- Assim como a ética, a segurança deve ser compreendida como parte fundamental da Cultura interna da **APET**., ou seja, qualquer incidente de segurança, subentende-se como alguém agindo contra a ética e os bons costumes regidos pela **APET**.
- A qualquer tempo e em qualquer dos casos previstos, prevalecendo o descumprimento das regras expostas a área de Suporte de TI poderá bloquear temporariamente o acesso do colaborador comunicando ao mesmo e ao gestor da área os motivos de tal ato. No caso de colaborador externo deverá ser comunicado ao responsável da empresa terceirizada.
- Esta PSI compromete e responsabiliza cada um, estando todos cientes também que os ambientes, telefones, sistemas, e-mails, computadores e redes da empresa estão sujeitos a monitoramento e gravação.
- É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do Departamento de compliance, do seu gestor ou da área de Suporte de TI, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.
- O colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de

suas funções na **APET**, mesmo após o encerramento do vínculo contratual mantido com a instituição.

18. CONTROLES INTERNOS

Ficam sujeitas a revisão, por parte de área de Controles Internos, a efetividade dos controles-chave sobre os processos descritos nesta política e revisão da avaliação dos riscos mais relevantes, através de metodologia própria representada pelo Perfil de Risco da Companhia com aprovação pela Diretoria da **APET** e alinhados a Estrutura de Gerenciamento de Riscos da companhia.

19. BASE NORMATIVA

- LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) 13.709
- ABNT NBR ISO/IEC 27002:2005
- DECRETO LEI QUE INSTITUI A POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO 9.637

20. ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política Segurança da Informação terá o prazo de 1 (um) ano para que possam ser realizadas as devidas atualizações e adequações para melhorias. Haverá exceção no prazo de atualização nos casos de exclusões, inclusões e/ou alterações dos conteúdos desta Política.

Data da última atualização: 07/05/2026

Versão do documento: 4

HISTÓRICO DE REVISÕES					
Versão Nº	**Data**	**Descrição da Alteração**	**Criado/ Modificado por**	**Revisado por**	**Aprovado por**
1º	01/07/2021	Elaboração	KRL Consultoria	Luiz Gênova – CEO	Luiz Gênova – CEO
2°	01/07/2023	Atualização	André Aguiar – AW3 Soluções Administrativas	Márcio Castro – Next Level Info	Luiz Gênova – CEO
3º	16/12/2024	Atualização	Karina Gregorio – Compliance APET	Guilherme Drigo – Next Level Info	Luiz Gênova – CEO
4º	07/05/2024	Atualização	Karina Gregorio – Compliance APET	Edmar Primio – TI e SI	Luiz Gênova – CEO

AP-POL003 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - versão IV pdf

Código do documento 2dfbaabc-4daa-46f7-bd2d-b5c53a6f129b

Assinaturas

Luiz Claudio de Gênova
luiz.genova@amigoopet.com.br
Assinou

Karina Cristine Gregorio
karina.gregorio@apetsaude.com.br
Assinou

Edmar Primio
edmar.primio@apetsaude.com.br
Assinou

Eventos do documento

18 May 2026, 14:04:28
Documento 2dfbaabc-4daa-46f7-bd2d-b5c53a6f129b **criado** por LUIZ CLAUDIO DE GÊNOVA (3ea87502-7767-4380-b8f5-f8c9d1af84b2). Email:luiz.genova@amigoopet.com.br. - DATE_ATOM: 2026-05-18T14:04:28-03:00

18 May 2026, 14:06:49
Assinaturas **iniciadas** por LUIZ CLAUDIO DE GÊNOVA (3ea87502-7767-4380-b8f5-f8c9d1af84b2). Email: luiz.genova@amigoopet.com.br. - DATE_ATOM: 2026-05-18T14:06:49-03:00

18 May 2026, 14:07:28
LUIZ CLAUDIO DE GÊNOVA **Assinou** (3ea87502-7767-4380-b8f5-f8c9d1af84b2) - Email: luiz.genova@amigoopet.com.br - IP: 177.55.197.95 (177-55-197-95.static.sumicity.net.br porta: 39210) - Geolocalização: -23.7628212655432 -45.723854935234705 - Documento de identificação informado: 051.117.598-16 - DATE_ATOM: 2026-05-18T14:07:28-03:00

18 May 2026, 14:28:14
EDMAR PRIMIO **Assinou** - Email: edmar.primio@apetsaude.com.br - IP: 191.177.160.251 (bfb1a0fb.virtua.com.br porta: 31554) - Geolocalização: -25.453791073468512 -49.21241099389594 - Documento de identificação informado: 713.844.809-00 - DATE_ATOM: 2026-05-18T14:28:14-03:00

18 May 2026, 14:33:13
KARINA CRISTINE GREGORIO **Assinou** - Email: karina.gregorio@apetsaude.com.br - IP: 45.190.158.88 (connectlinksp.com.br porta: 7374) - Geolocalização: -23.663725954955016 -46.761610929357055 - Documento

de identificação informado: 488.991.028-05 - DATE_ATOM: 2026-05-18T14:33:13-03:00

Hash do documento original

(SHA256):0ee5ab374c2525d04ddb9dc7cadf4b202fa5d55e9b2e7d05d29f24c87efb602d
(SHA512):141be57cfe9e84c150a0320f10ba78bebe7e77941e66bad8c1acf843ae3e86715c2cd68406844c361d1634b99e94d02c16a5a166d8e9a020d6675d9019113d8e

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.