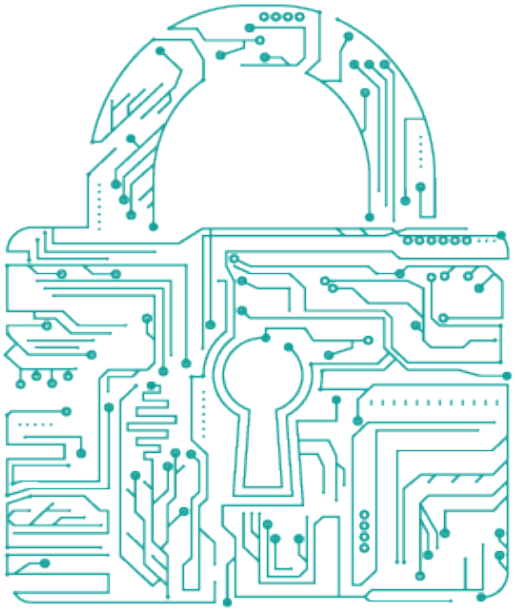
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Administração Municipal - Gestão 2020-2024

Rubens Bomtempo

Prefeito

Paulo Mustrangi

Vice-Prefeito

Claudinei Portugal

Diretor-Presidente

Flávio Holanda

Chefe de Tecnologia da Informação

Nerthan Buarque

Técnico de Processamento de Dados

Política de Segurança da Informação
Versão 1.0 - Maio/2023

Sumário

Apresentação

Esta Política de Segurança da Informação (“Política de Sistema de Informação”) é uma declaração formal, aprovada pelo INPAS, comunicada a todos os colaboradores e, sempre que cabível, as partes externas relevantes, acerca do compromisso deste ente em adotar seus melhores esforços para garantir a preservação da segurança dos serviços, recursos, dados pessoais e das demais informações geridas dentro de sua infraestrutura física e de Tecnologia da Informação (“TI”).

Esta Política de Sistema de Informação e todas as normas e procedimentos a ela conexos se aplicam a todos os usuários de sistemas, do site, aplicativos e redes sociais do INPAS, prestadores de serviços, fornecedores e agentes públicos.

A Política de Sistema de Informação é revisada e atualizada periodicamente, com prazo de no mínimo 2 (dois) anos e sempre que os procedimentos de manutenção, análise crítica e melhoria no Sistema de Gestão da Segurança da Informação (SGI) do INPAS demandem alterações significativas, com o objetivo de assegurar sua contínua pertinência, adequação e eficácia no alcance dos objetivos propostos.

É responsabilidade de cada parte interessada, seja ela interna ou externa, consultar sempre a versão mais atualizada da Política de Sistema de Informação quando houver qualquer questão referente aos temas nela tratados.

Esta Política deverá ser publicada em cada revisão no meio de publicação oficial do INPAS, bem como no sítio eletrônico, com fácil acesso.

OBJETIVO - Estabelecer diretrizes para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, bem como a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade, autenticidade das informações no INPAS, e a continuidade dos seus negócios.

ABRANGÊNCIA – Todos, Diretor-Presidente, Diretores, Coordenadores, Colaboradores, Estagiários, Fornecedores e Prestadores de Serviços, bem como toda pessoa física ou jurídica que, de alguma forma, executem atividades funcionais amparadas por contratos ou instrumentos jurídicos e que, para tanto, venham a utilizar ou ter acesso às informações de propriedade do INPAS ou sob sua custódia, em qualquer meio, especialmente, físico ou eletrônico.

1. Definições

Para os efeitos desta Política de Sistema de Informação, aplicam-se os seguintes termos e definições:

1.1. **Aceitação do risco:** decisão de quem detenha competência de acordo com o Estatuto Social e normas internas do INPAS quanto à aceitação de um risco;

1.2. **Agente público:** servidores estatutários, comissionados, agentes políticos, empregados públicos, estagiários e terceirizados;

1.3. **Análise/avaliação de riscos:** processo completo de análise e avaliação de riscos;

1.4. **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;

1.5. **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento dos dados pessoais,

por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

1.6. **Autenticação em dois fatores ou sistema de dupla verificação:** medida de segurança para evitar o uso indevido de senhas, exigindo que o usuário forneça, além da senha, outra informação, preferencialmente, que apenas ele tenha a resposta;

1.7. **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da Administração Pública federal, ao qual se refere o art. 55-A e seguintes da LGPD, responsável por zelar pela proteção de dados pessoais, estabelecer diretrizes, fiscalizar e aplicar sanções;

1.8. **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

1.9. **Ativo:** qualquer bem ou direito pertencente o INPAS e que possa ser convertido em dinheiro;

1.10. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados, e que gera a obrigação de preservá-la;

1.11. **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;

1.12. **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

1.13. **Disponibilidade:** propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;

1.14. **Oficial de Proteção de Dados (OPD) ou encarregado de proteção de dados pessoais:** a pessoa indicada, nos termos da “Política de Privacidade” do INPAS, para atuar como canal de comunicação com os contratantes, os titulares dos dados pessoais e a ANPD;

1.15. **Evento de Segurança da Informação:** uma ocorrência identificada de um estado de sistema, serviço ou rede,

indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

1.16. **Gestão de riscos:** atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

1.17. **Incidente de Segurança da Informação:** um ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

1.18. **Integridade:** propriedade de salvaguarda da exatidão e abrangência de ativos, assegura que a informação não seja modificada de forma indevida ou destruída de maneira não autorizada, seja de forma intencional, seja acidental;

1.19. **Lei Geral de Proteção de Dados (LGPD):** Lei nº 13.709, de 14 de agosto de 2018;

1.20. **Política de Privacidade:** política do INPAS que disciplina o tratamento de dados pessoais, com vistas a proteger a privacidade dos titulares dos dados pessoais, tais como os usuários dos serviços do INPAS e colaboradores. A Política de Privacidade está disponível para consulta no site do INPAS e sua intranet;

1.21. **Segurança da Informação:** preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

1.22. **Sistema de Gestão da Segurança da Informação (SGSI):** parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Inclui estrutura organizacional, políticas, normas e procedimentos, atividades de planejamento, responsabilidades, práticas, processos e recursos;

1.23. **Tratamento de dados:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

1.24. **Tratamento do risco:** processo de seleção e implementação de medidas para modificar um risco;

1.25. **Titular de dados pessoais:** pessoa natural a quem se refere os dados pessoais que são objeto de tratamento.

2. Princípios da Segurança da Informação

Para garantir a segurança da informação, o INPAS, na execução de sua atividade, se baseia nos seguintes princípios:

2.1. **Confidencialidade:** Somente pessoas devidamente autorizadas devem ter acesso à informação;

2.2. **Integridade:** É vedada a manipulação das informações, portanto, são proibidas alterações, supressões e adições de conteúdo nas informações, salvo se expressamente autorizadas;

2.3. **Disponibilidade:** A informação deve estar disponível para as pessoas autorizadas, sempre que necessário ou demandado;

2.4. **Rastreabilidade:** Possibilita acompanhar ou identificar o percurso de um dado ou informação durante um processo: saber onde, como, por quem e quando o dado foi manipulado/acessado;

2.5. **Conformidade:** Toda a Política de Segurança de Informação deverá estar em conformidade com as boas práticas estabelecidas, bem como às normas legais em vigência (LGPD e LAI).

3. Objetivos

Esta Política de Sistema de Informação tem por objetivos:

3.1. Estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos de informação;

3.2. Implementar controles e procedimentos para reduzir a vulnerabilidade do INPAS a incidentes de segurança da informação;

3.3. Apoiar a alta direção na implementação da Gestão de Segurança da Informação;

3.4. Prover os colaboradores e partes externas relevantes com orientação e apoio da Direção do INPAS, para a garantia da Segurança da Informação, de acordo com os requisitos das atividades desempenhadas pelo INPAS e com as leis e regulamentações aplicáveis;

3.5. Implementar controles buscando a disponibilidade, integridade, confidencialidade, segurança e autenticidade dos dados e das informações tratadas.

4. Classificação da Informação

Os titulares das unidades organizacionais do INPAS são responsáveis por alocar a informação que transita por sua área conforme a classificação abaixo, responsabilizando-se por tal alocação e fornecendo as orientações pertinentes à sua equipe. As informações serão classificadas entre:

4.1. Informação Pública: toda informação que possa ser acessada por usuários da organização, fornecedores, prestadores de serviços e público em geral. São informações que são divulgadas pelo INPAS de forma pública e que podem ser acessadas por terceiros sem qualquer restrição ou necessidade de sigilo;

4.2. Informação Interna: toda informação que possa ser acessada apenas por colaboradores da organização, independentemente do pertencimento a uma área específica. São sigilosas em relação ao público, seja porque poderiam comprometer a imagem da organização, seja por razões estratégicas sobre as atividades desempenhadas, incluindo,

ainda informações relativas aos clientes, fornecedores e prestadores de serviços;

4.3. Informação Restrita: toda informação que possa ser acessada apenas por colaboradores da organização, desde que explicitamente indicados pelo nome ou pela área a que pertencem. São sigilosas em relação público e também aos colaboradores vinculados às demais áreas do INPAS que não estejam expressamente autorizadas a acessá-las;

4.4. Informação Confidencial: toda informação que possa ser acessada apenas por colaboradores da organização, desde que explicitamente indicados pelo nome ou pela área a que pertencem e desde que tenham inequívoca necessidade de conhecimento da informação para o desempenho de alguma de suas funções. Inserem-se nessa categoria também os dados pessoais de colaboradores, prestadores de serviços e de usuários dos serviços do INPAS. São sigilosas em relação ao público e também aos colaboradores vinculados às demais áreas do INPAS que não tenham expressa necessidade de acessá-las para desempenhar suas funções;

4.5. A classificação das informações conforme o item 4.4 acima gera para os colaboradores e quaisquer pessoas que tenham acesso a informações do INPAS, a obrigação de preservá-las nos termos previstos, mantendo o seu sigilo em relação aos grupos de pessoas identificados acima;

4.6. Os titulares das unidades organizacionais do INPAS devem orientar sua equipe a tratar a Informação Restrita e a Informação Confidencial como se fossem seus próprios dados sigilosos, destacando que a divulgação não autorizada pode causar sérios danos às atividades do INPAS e/ou comprometer a atuação da organização;

4.7. Os dados pessoais deverão, independentemente de qualquer indicação, ser sempre considerados como Informação Confidencial, de modo que colaboradores que tenham acesso a tais dados deverão zelar pelo sigilo dessas informações e não poderão transferi-las a terceiros sem expressa autorização do titular, tampouco a colaboradores do INPAS que não tenham expressa necessidade de acessá-las para fins de cumprimento de suas funções.

5. Armazenamento de Informações em Suporte Físico

As informações em suporte físico deverão ser armazenadas em local apropriado, sendo que as classificadas como internas, restritas ou confidenciais devem estar protegidas de acesso indevido por meio de chave e com controle de retirada e devolução.

6. Obrigações dos Colaboradores

Todos os colaboradores são responsáveis por proteger a informação contra qualquer acesso não autorizado.

6.1. A obrigação de confidencialidade inclui o dever de, considerados o conteúdo e a finalidade das informações, não compartilhá-las com pessoas que não tenham expressa autorização para acessá-las nos termos da Cláusula 6 acima e, na hipótese de não haver clareza quanto ao tipo de informação acessada, não compartilhá-la com quem não tenha necessidade de acessá-la para o desempenho de suas funções dentro do INPAS, preservando-se, entretanto, o direito dos titulares de dados pessoais de acessar suas próprias informações. Referente aos dados sediados em servidores, os proprietários dos dados ficam obrigados a anualmente revisar a lista de usuários com os permissionamentos;

6.2. É obrigação dos colaboradores zelar para que a integridade da informação seja mantida. A obrigação de preservação da integridade das informações inclui o dever de abster-se de promover qualquer alteração do conteúdo das informações ou de descartá-las sem observância dos procedimentos exigidos ou fora das hipóteses em que o descarte objetive o cumprimento das finalidades de manutenção da segurança da informação;

6.3. É dever dos colaboradores zelar para que seja mantida a disponibilidade da informação para os processos e atividades do INPAS;

6.4. O dever de manter a disponibilidade inclui a vedação a que informações sejam mantidas fora dos ambientes eletrônicos ou físicos a elas destinados, ou que seu depósito ou armazenamento seja feito com restrição que impeça o acesso a quem tenha o dever de acessar as respectivas informações;

6.5. Na hipótese de suspeita de violação a qualquer norma contida nesta Política de Sistema de Informação ou incidente de segurança, os colaboradores têm obrigação de comunicar imediatamente o titular da unidade organizacional;

6.6. Caso se trate de situação que envolva Tecnologia da Informação, incluindo, mas não se limitando a perda de senha, invasões de sistemas e situações semelhantes, o colaborador deve reportar o ocorrido ao departamento responsável por Tecnologia da Informação;

6.7. É obrigação do titular da unidade organizacional acompanhar o tratamento da questão junto ao departamento responsável por Tecnologia da Informação;

6.8. É obrigação do departamento responsável por Tecnologia da Informação reportar ao titular da unidade organizacional e à Diretoria de Gestão Corporativa do INPAS sobre os tratamentos conferidos;

6.9. Caso se trate de problema que envolva dados pessoais, os colaboradores, incluindo os titulares das unidades organizacionais e o departamento responsável por Tecnologia da Informação, devem reportar o ocorrido simultaneamente ao DPO e ao titular da unidade organizacional.

7. Penalidades

7.1. Nenhum colaborador poderá, sob qualquer circunstância, alegar o desconhecimento desta Política de Sistema de Informação para justificar eventuais violações ou inobservância aos termos nela previstos, ainda que por omissão ou falta nos deveres de cuidado descritos;

7.2. A inobservância às regras e aos procedimentos estabelecidos e implícitos nesta Política de Sistema de Informação poderá sujeitar o infrator e aqueles que com ele colaborarem, às sanções previstas nas regulamentações internas do INPAS, no Código de Conduta e Integridade, na legislação vigente, bem como no contrato pelo qual estejam vinculados o INPAS, sem prejuízo da aplicação de outras sanções administrativas ou legais, cíveis ou criminais, bem como de ações por reparação de eventuais perdas e danos que o INPAS venha a enfrentar em decorrência da violação;

8. Política de Controle de Acesso

8.1. O Controle de Acesso envolve o acesso lógico, aos recursos de tecnologia e o acesso físico às instalações do INPAS;

8.2. O Controle de Acesso à informação, bem como a quaisquer bens e equipamentos ou qualquer suporte físico que contenha informações, deve considerar os seguintes aspectos:

8.2.1. Todo uso de informação deve observar as normas desta Política de Sistema de Informação, devendo ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário;

8.2.2. É obrigatória a prévia autorização da área proprietária dos dados, caso seja necessário o acesso a dados complementares não originalmente pertinentes à área de atuação do colaborador, o que deverá ocorrer mediante identificação única e intransferível do usuário;

8.2.3. Sempre que houver a admissão ou mudança das atribuições do usuário, o acesso a novas informações deve ser autorizado pelo superior imediato, para que a unidade organizacional responsável pela Tecnologia da Informação providencie as permissões de acesso compatíveis, bem como demais providências necessárias;

8.2.4. Sempre que houver mudança de alocação do usuário, o acesso às informações da área de origem deverá ser automaticamente bloqueado pela unidade organizacional responsável pela Tecnologia da Informação. O acesso às novas informações na área de destino deve ser autorizado pelo superior imediato, para que a unidade organizacional responsável pela Tecnologia da Informação providencie as permissões de acesso compatíveis, bem como demais providências necessárias;

8.2.5. A unidade organizacional responsável pela administração de pessoal comunicará à unidade organizacional responsável pela Tecnologia da Informação sempre que houver movimentação de funcionários para o respectivo bloqueio.

8.2.6. Sempre que houver desligamento de colaboradores, a unidade organizacional responsável pela Tecnologia da Informação deverá imediatamente recolher os equipamentos, observado o item 8.2.7 abaixo, bens e quaisquer informações utilizadas pelo colaborador e remover imediatamente o acesso do usuário aos sistemas do INPAS;

8.2.7. Caso o colaborador utilize equipamentos próprios, deverá entregá-los à unidade organizacional responsável pela Tecnologia da Informação, para remoção das informações pertinentes ao INPAS;

8.2.8. A unidade organizacional responsável pela administração de pessoal deverá providenciar a notificação à unidade organizacional responsável pela Tecnologia da Informação quanto aos ajustes necessários dos privilégios de acesso aos sistemas e equipamentos, bem como a adequação em relação aos acessos físicos;

8.3. O Controle de Acesso Físico às instalações do INPAS é monitorado, apenas sendo autorizada a entrada de colaboradores, prestadores de serviço e usuários dos serviços, podendo, conforme o caso, ser autorizada a entrada de acompanhante dos usuários e, ainda:

8.3.1. A entrada e permanência de usuários e respectivos acompanhantes deve ser sempre acompanhada por colaborador do INPAS da área onde atuará o prestador de serviço;

8.3.2. A entrada e permanência de prestadores de serviços eventuais deve ser sempre supervisionada por colaborador do INPAS da área onde atuará o prestador de serviço;

8.3.3. Os colaboradores devem evitar acessar áreas do INPAS às quais o acesso não seja necessário ao desempenho de suas atividades.

8.4. O Controle de Acesso Lógico aos equipamentos e computadores do INPAS, bem como à rede interna e aos seus sistemas de dados, é realizado por intermédio de senhas que garantam acesso adequado a cada perfil de acesso e respectivos privilégios, e cuja definição e utilização devem

observar a Política de Senhas descrita na Cláusula 11 desta Política de Sistema de Informação.

8.5. O titular da unidade organizacional é responsável por comunicar a DTI pela conformidade e gestão de riscos do INPAS sobre toda e qualquer infração a esta Política de Sistema de Informação, incluindo as suspeitas, sob pena de incorrer pessoalmente nas penalidades previstas no item 8.4 acima.

9. Coordenação de Segurança da Informação

São designados os seguintes "Coordenadores de Segurança da Informação", responsáveis pelo gerenciamento e aplicação da Política de Sistema de Informação em cada área do INPAS:

Coordenador	Atribuições Centrais
Agentes Políticos (Diretores)	● Mapear as demandas internas, abrangendo os requisitos da legislação vigente e as especificações dos produtos e serviços, para oferecer soluções tecnológicas compatíveis às necessidades da empresa; ● Procurar sempre a atualização tecnológica necessária, conforme às tendências de inovação e ofertas dos principais provedores de softwares, hardwares e serviços de tecnologia, para atender de forma proativa com soluções tecnológicas que promovam melhorias operacionais e ganho de performance nos processos corporativos da secretaria; ● Implantar todas as práticas abrangentes aos ativos de tecnologia e segurança de informação desta norma nos

	diversos setores sobre sua responsabilidade.
Responsável pela TI da Unidade	• Informar e aconselhar o responsável pelo tratamento e os demais profissionais sobre suas obrigações nos termos da LGPD; • Controlar a conformidade com as políticas do responsável pelo tratamento, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido no tratamento; • Prestar aconselhamento, se tal for solicitado, no que se refere à avaliação do impacto da proteção de dados, e acompanhar o seu desempenho; • Cooperar com as autoridades; • Servir de ponte para a autoridade de supervisão em questões relacionadas com o tratamento.
Colaboradores das Unidades	• Auxiliar ao INPAS na adequação de processos, procedimentos de registro e controles internos para atendimento dos princípios da LGPD; • Revisar documentos no intuito de resguardar os direitos das pessoas quanto a eventuais incidentes de privacidade.

10. É competência comum dos Responsáveis pela TI da Unidade

a) Fornecer aos colaboradores os esclarecimentos necessários sobre quaisquer questões referentes aos temas tratados nesta Política de Sistema de Informação, devendo buscar as respostas que eventualmente não se sintam habilitados a responder junto ao responsável pelas iniciativas de segurança;
b) Receber eventuais denúncias realizadas por colaboradores acerca de potenciais infrações, eventos ou incidentes de segurança da informação, e encaminhá-los a investigação e mitigação de danos, nos termos previstos na Política de Privacidade, mantendo os registros das denúncias recebidas e do tratamento aplicado;
c) Comunicar imediatamente o DPO, sempre que alguma denúncia envolva potenciais eventos ou incidentes com dados pessoais;
d) Controlar a necessidade de compartilhamento de informações em sua área, devendo, sempre que cabível, celebrar acordos de confidencialidade.

Sempre que verificado que as medidas necessárias à mitigação de um risco são muito onerosas, a decisão quanto à aceitação do risco é competência exclusiva do Gestor do Órgão, observado o estabelecido em seu Estatuto Social.

11. Política de Senhas

11.1 As senhas iniciais são definidas no ato da admissão do colaborador, pela unidade organizacional responsável pela administração de pessoal no momento de criação do usuário no sistema utilizado, após assinatura de Termo de Responsabilidade, devendo ser alteradas no momento do primeiro acesso.

a) A criação de usuário e senha para terceiros será feita pela unidade organizacional responsável pela Tecnologia da Informação, mediante a assinatura de Termo de Responsabilidade.

11.2 A senha será de uso individual, pessoal, intransferível e de responsabilidade exclusiva do colaborador a quem se vincula.

11.3 As senhas são pessoais e devem ser protegidas pelos colaboradores, não podendo ser transferidas a terceiros e, ainda:

a) Cada colaborador é exclusivamente responsável pela confecção e confidencialidade de sua senha de conta de acesso, bem como por zelar pelo uso correto de sua identificação. Os atos praticados por terceiros serão de

responsabilidade dos colaboradores cujo acesso estiver habilitado no equipamento.

b) As senhas não poderão ser divulgadas, cedidas e/ou compartilhadas, ou ainda mantidas escritas ou armazenadas, manualmente ou digitalmente, sem mecanismos adequados de proteção homologados pela unidade organizacional responsável pela Tecnologia da Informação.
c) Não é permitida a gravação de senhas para serem automaticamente utilizadas por programas, sistemas, serviços e computadores.

11.4 Caso o colaborador perca a senha ou desconfie do acesso ao seu equipamento por terceiros deverá informar imediatamente a unidade organizacional responsável pelo sistema em questão, que providenciará a troca da mesma.

12. Acesso Remoto (VPN)

12.1 O acesso remoto de uma rede externa às estações de trabalho do INPAS deverá ser monitorado, autorizado e somente feito utilizando VPN.

12.2 Somente será fornecido acesso a VPN para colaboradores ou prestadores de serviço em regime de trabalho remoto ou cujas atividades possam demandar acesso à rede interna do INPAS quando estejam fora das instalações físicas da organização, ou ainda em casos específicos, a colaboradores que utilizem dispositivos próprios.

12.3 O acesso remoto deve ser solicitado a unidade organizacional responsável pela Tecnologia da Informação, com a justificativa fundamentada.

12.4 Os usuários que tiverem direito ao acesso remoto devem estar cientes de que:

a) A proteção da confidencialidade das informações nos equipamentos utilizados para acesso ao VPN é de responsabilidade do próprio usuário.
b) Os recursos de Tecnologia da Informação, disponibilizados têm como objetivo a realização de atividades profissionais, respeitando o horário normal de expediente e as prorrogações de jornada autorizadas.
c) O usuário com acesso remoto autorizado, acessa os mesmos ambientes que visualiza internamente, ou seja, manterá o

perfil de acesso que detém quanto dentro das instalações físicas do INPAS.

12.5 Os usuários autorizados ao acesso remoto, devem garantir que seu perfil de acesso remoto não seja utilizado por outras pessoas, protegendo suas credenciais e, em nenhum momento, devem disponibilizar seu login e senha VPN, ou qualquer informação de acesso a terceiros.

13. Teletrabalho

13.1 Os colaboradores em regime de teletrabalho ou que sejam autorizados a realizar todas as atividades à distância assumem o compromisso de:

a) Manter sempre instalados e atualizados softwares de segurança como antivírus e firewalls;
b) Realizar verificação por antivírus em todo arquivo em mídia proveniente de entidade externa e/ou recebido/obtido pela internet;
c) Não conectar seu dispositivo a redes Wi-Fi não criptografadas;
d) Não enviar documentos da organização para sua conta de e-mail pessoal, tampouco realizar quaisquer tipos de cópias dos documentos, devendo solicitar autorização para imprimir quaisquer materiais, mediante justificativa quanto à necessidade;
e) Não publicar fotos do ambiente de trabalho remoto em redes sociais expondo dados e sistemas da organização;
f) Dedicar o máximo cuidado com a segurança física do equipamento utilizado, seja pessoal, seja fornecido pelo INPAS, bem como ao acesso ou visualização de informações por terceiros;
g) Autorizar que a unidade organizacional responsável pela Tecnologia da Informação realize revisões periódicas nos equipamentos utilizados, de modo a garantir a atualização de sistemas de segurança, inclusive antivírus e firewalls, bem como para fins de auditoria referente à adequada utilização dos sistemas do INPAS, com vistas a assegurar o mesmo nível de segurança aplicado aos equipamentos utilizados dentro das instalações do INPAS.

14. Traga seu próprio dispositivo “Bring your own device” (BYOD)

14.1 A utilização de dispositivos de propriedade pessoal (BYOD), inclusive dispositivos móveis como smartphone, ultrabook, notebook, tablet etc., é permitida, nos seguintes termos:

a) O acesso exclusivo à Internet, inclusive por prestadores de serviços e usuários dos serviços do INPAS, bem como acompanhantes, poderá ser feito sem o cadastro prévio do dispositivo BYOD através de redes sem fio configuradas com restrições de segurança e que não permitirão o acesso aos demais serviços de TIC (por exemplo: VoIP, Impressão, sistemas internos, etc), mediante comunicação prévia com o Setor de Tecnologia da Informação e Proteção de Dados;
b) A unidade organizacional responsável pela Tecnologia da Informação poderá, sem aviso prévio, suspender o acesso em caso de suspeita de incidentes de segurança da informação. Nesses casos, o dispositivo estará sujeito à coleta de informações de hardware e software exclusivamente através da coleta de tráfego da rede interna ou externa, ressalvada a privacidade do usuário.
c) Em casos de comprovação de incidentes de segurança da informação envolvendo dispositivo BYOD, o acesso será revogado e serão tomadas as devidas providências administrativas para apuração da responsabilidade.
d) Os softwares utilizados nos dispositivos BYOD deverão possuir licenças válidas, estando o usuário ciente de que a violação de direito autoral relacionado a softwares configura crime tipificado pela legislação brasileira.
e) O usuário será o único responsável pela manutenção e atualização das licenças dos softwares instalados no seu dispositivo e responderá por qualquer incidente ou demanda sobre o uso de software não licenciado em seu dispositivo.
f) É responsabilidade do usuário, a guarda e manutenção adequada do dispositivo BYOD, bem como a segurança dos dados armazenados no dispositivo, sendo o proprietário responsável por eventuais vazamentos de informações ou perda de dados. Recomenda-se a utilização de criptografia nos dados do dispositivo e backup frequente dos dados, bem como o uso de software de Antivírus/Firewall.
g) O INPAS não se responsabiliza por acessos indevidos ao dispositivo ou danos de hardware e/ou software que possam ocorrer, mesmo quando o dispositivo for utilizado para acesso à rede INPAS ou execução das atividades do usuário.
h) Em caso de perda, roubo ou furto do dispositivo credenciado, a unidade organizacional responsável pela Tecnologia da Informação deverá ser informada imediatamente, via sistema de chamado ou email, para que sejam tomadas as medidas

de segurança cabíveis, com o descredenciamento objetivando evitar o uso indevido do dispositivo extraviado por terceiros dentro do ambiente do INPAS.

i) Qualquer utilização de dispositivos BYOD para atividades além do exclusivo acesso à rede destinada a visitantes estará sujeita às demais regras previstas nesta Política de Sistema de Informação.

15. Utilização de Computador/Notebook do INPAS

15.1 O uso dos computadores e notebooks é restrito às atividades profissionais do usuário, observado o horário normal de expediente e as prorrogações de jornada autorizadas.

15.2 Somente funcionários ou prestadores de serviços com usuário e senha válidos podem acessar os computadores do INPAS.

15.3 Para o acesso a sistemas da organização é obrigatória a utilização de senha pessoal do colaborador.

15.4 Nenhum usuário deverá possuir perfis e privilégios de acesso diferente da área em que atua.

15.5 A unidade organizacional responsável pela Tecnologia da Informação deve ser imediatamente comunicada pelos Coordenadores e/ou unidade organizacional responsável pela administração de pessoal sempre que houver alteração do perfil de acesso dos usuários ou sua retirada em caso de desligamento.

15.6 A utilização de notebooks do INPAS está condicionada a que o colaborador assine o Termo de Responsabilidade para Uso de Aparelhos.

a) O INPAS poderá, a seu exclusivo critério e a qualquer tempo, mesmo durante a vigência do contrato que estabeleça o vínculo com o colaborador, suspender, interromper ou cessar o fornecimento dos equipamentos, seus acessórios e serviços agregados, independentemente de qualquer motivação ou justificativa prévia, sem direito a qualquer reparação por parte do usuário.

b) Finda a relação contratual entre o INPAS e o colaborador, os equipamentos e seus acessórios deverão ser devolvidos ao INPAS no exato estado em que foram cedidos ao usuário, com

exceção do desgaste natural decorrente do uso, sob pena de ressarcimento pelo usuário ao INPAS do valor correspondente aos danos causados.

15.7 Os equipamentos disponibilizados para o uso dos colaboradores são de propriedade ou de responsabilidade da organização, cabendo aos colaboradores utilizá-los e manuseá-los corretamente para as atividades de interesse do INPAS e exercício de suas atividades e, portanto, é obrigação de cada usuário:

a) Utilizar o equipamento com zelo e manter a boa conservação do aparelho, responsabilizando-se pela perda e eventuais avarias que o equipamento venha a sofrer;
b) Responsabilizar-se pelos equipamentos que esteja autorizado a utilizar e seus respectivos acessórios, de modo que não poderá trocá-los, permutá-los ou emprestá-los a outros usuários, sem prévia e expressa autorização do INPAS;
c) Suportar integralmente os danos de qualquer natureza causados ao equipamento e seus acessórios, em decorrência de mau uso;
d) Reportar à unidade organizacional responsável pela Tecnologia da Informação do INPAS quaisquer comportamentos suspeitos do equipamento ou dos sistemas, para que possíveis falhas ou incidentes, inclusive vírus, possam ser identificados no menor tempo possível;
e) informar à equipe da unidade organizacional responsável pela Tecnologia da Informação qualquer identificação de dispositivo estranho conectado ao seu computador.

15.8 É proibida e, sempre que possível, será barrada pelos sistemas, podendo sujeitar o usuário a medidas de responsabilização e reparação de danos:

a) Utilização de todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos sistemas dos computadores e notebooks, sem o conhecimento prévio e o acompanhamento da unidade organizacional responsável pela Tecnologia da Informação do INPAS;
b) Realização de reparo de computadores/notebook ou outros equipamentos de informática por qualquer pessoa que não seja da unidade organizacional responsável pela Tecnologia da Informação do INPAS ou terceiro devidamente contratado para o serviço;

c) Instalação ou uso de software nos equipamentos sem a expressa autorização e acompanhamento da unidade organizacional responsável pela Tecnologia da Informação;
d) Utilização de pen-drive, devendo o usuário solicitar à unidade organizacional responsável pela Tecnologia da Informação a cópia do conteúdo para uma pasta de rede exclusivamente nas hipóteses em que a cópia seja autorizada pelo titular da unidade organizacional correspondente, devendo ser adequadamente motivada;
e) Utilização de pastas públicas ou outras cujo acesso não seja restrito, para armazenamento de arquivos que contenham Informação Confidencial ou Informação Restrita.

15.9 O INPAS respeita os direitos autorais dos programas e não autoriza o uso de programas não licenciados nos computadores da entidade. Portanto, é terminantemente proibido o uso de programas ilegais (sem licenciamento) ou não autorizados pelo INPAS.

a) A instalação de quaisquer softwares, drivers e/ou programas apenas poderá ser realizada pela unidade organizacional responsável pela Tecnologia da Informação do INPAS, desde que alinhados à Política de Sistema de Informação e que não representem risco ao SGSistema de Informação do INPAS.
b) A unidade organizacional responsável pela Tecnologia da Informação fará verificações periódicas nos dados dos servidores e/ou computadores e notebook dos usuários, visando garantir a correta aplicação dessa diretriz.
c) Caso sejam encontrados programas não autorizados, estes deverão ser removidos imediatamente, e o usuário será devidamente responsabilizado.
d) Os sistemas de Tecnologia da Informação devem ser utilizados sem violação dos direitos de propriedade intelectual de qualquer terceiro.
e) Aqueles que instalarem tais programas não autorizados nos computadores ou violarem direitos de propriedade intelectual se responsabilizarão perante o INPAS por quaisquer problemas ou prejuízos causados em decorrência desta ação.

15.10 Os computadores/notebook deverão conter versões do software antivírus instaladas, ativadas e atualizadas permanentemente.

a) A atualização do antivírus será automática, agendada pela unidade organizacional responsável pela Tecnologia da Informação.

b) É expressamente proibido desabilitar o programa antivírus instalado nos equipamentos.
c) Todo arquivo em mídia proveniente de entidade externa ao INPAS deve ser verificado por programa antivírus, bem como todo arquivo recebido/obtido pela Internet.

15.11 Todos os computadores/Notebook utilizados para acessar sistemas do INPAS poderão:

a) Ser acessados remotamente somente pela unidade organizacional responsável pela Tecnologia da Informação.
b) Passar por auditorias interna/externa realizadas pela unidade organizacional responsável pela Tecnologia da Informação ou terceiro contratado pelo INPAS.
c) Ter as informações do seu registro de "log" do Sistema Operacional examinadas, para fins de acompanhamento, monitoramento e controle de sua utilização, visando, inclusive, à proteção do colaborador contra invasões indevidas.

16. Acesso à Internet

16.1 A internet deve ser utilizada para fins de complemento às atividades profissionais, para o enriquecimento intelectual dos colaboradores ou, no caso dos pesquisadores, como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

16.2 É expressamente vedada a utilização para realização de trabalhos de terceiros ou de atividades que tenham finalidade diversa daquela para qual o usuário foi contratado.

16.3 Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente à unidade organizacional responsável pela Tecnologia da Informação com prévia autorização do titular da unidade organizacional.

16.4 O uso da internet será auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

16.5 As seguintes atividades são proibidas:

a) Baixar arquivos como vídeos, imagens e executáveis da Internet que não foram aprovados pela unidade organizacional responsável pela Tecnologia da Informação;
b) Acessar sites com conteúdo pornográfico, webproxys, jogos, bate-papo, apostas e assemelhados. Tais conteúdos estarão bloqueados e serão monitorados, sujeitando o infrator que os acessar às penalidades cabíveis;
c) Utilizar softwares P2P que realizam buscas e baixem arquivos (download) de conteúdo de áudio, vídeo, programas etc. (por exemplo, torrents);
d) Acessar jogos online, rádio e TV online.

16.6 Todo o acesso a internet por meio de equipamentos do INPAS será monitorado através de logs contendo MAC, IP, URL acessada, data e horário, possibilitando o rastreio da atividade.

17. Uso de E-mail

17.1 A ferramenta de e-mail será fornecida de forma setorial ao secretário responsável pela unidade organizacional, a quem se atribui total responsabilidade sobre o seu uso, para uso exclusivo em suas atividades profissionais, podendo repassar para o uso de colaboradores sob a sua responsabilidade.

17.2 Os usuários devem:

a) Adotar o e-mail como recurso preferencial para comunicações oficiais internas que não necessitam ser circuladas por meio físico escrito, com vistas a reduzir o risco de exposição de papéis a terceiros, bem como o custo com impressão, aumentando a agilidade na entrega e leitura da informação;
b) Cuidar para que sua senha de acesso ao equipamento e ao e-mail não sejam acessadas por terceiros e bloquear os equipamentos quando não estiverem em uso, sendo o responsável direto pelas mensagens enviadas por seu endereço de e-mail;
c) Realizar a manutenção da caixa de e-mail, apagando mensagens inúteis e evitando acúmulo de informações desnecessárias.

17.3 Os usuários não devem:

a) Abrir e-mails de remetentes com os quais não estejam familiarizados;

b) Abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela unidade organizacional responsável pela Tecnologia da Informação, caso não tenha certeza absoluta de que solicitou o conteúdo;
c) Clicar em links, exceto quando tenha certeza absoluta de que solicitou o conteúdo ou quando confirmado com a unidade organizacional responsável pela Tecnologia da Informação que se trata de link confiável;
d) Abrir e-mails com assuntos estranhos, potencialmente nocivos e/ou em inglês, tendo em vista a gravidade de vírus circulados nos últimos anos por e-mails que continham assuntos maliciosos;
e) Utilizar o e-mail fornecido pelo INPAS para assuntos pessoais;
f) Utilizar o seu e-mail pessoal para enviar correntes para e-mails do INPAS;
g) Enviar anexos (arquivos) muito grandes, exceto quando estritamente necessário ao desempenho de suas atividades.

17.4 É proibido o envio de grande quantidade de mensagens de e-mail (spam), o que inclui mala direta, correntes, anúncios, propaganda política etc.

18. Uso de aplicativos de mensagens (whatsapp, telegram etc.)

18.1 Quando for necessário utilizar aplicativos de mensagens, como WhatApp, Telegram ou equivalentes, para tratar assuntos que envolvam as atividades profissionais, os colaboradores:

a) Devem ter habilitado a autenticação em dois fatores para acesso ao aplicativo a ser utilizado;
b) São obrigados a conferir às informações exatamente o mesmo nível de cuidado e de confidencialidade empregado dentro das instalações e por meio dos sistemas e equipamentos do INPAS;
c) São proibidos de criar grupos com o nome ou logo INPAS, exceto quando expressamente autorizado pelo titular da unidade organizacional à qual o colaborador está vinculado, mediante justificativa quanto à necessidade do grupo;
d) Não devem postar mensagens com conteúdo humorístico, pornográfico, religioso, racista ou que expresse preconceito de qualquer natureza, correntes, ou ativismo político, bem como qualquer outro tipo de conteúdo que viole o Código de Conduta e Integridade;

e) É proibido disponibilizar qualquer tipo de documento de quaisquer usuários dos serviços do INPAS, tampouco de qualquer colaborador da organização ou prestador de serviço.

19. Política Mesa Limpa e Tela Protegida

19.1 Os colaboradores e todos que tenham acesso físico ou lógico ao INPAS devem adotar a política “Mesa limpa e Tela Protegida”, para minimizar os riscos de acesso não autorizado, perda ou corrompimento de informações durante e fora do horário de expediente.

19.2 A política de “Mesa Limpa” é aplicada no ambiente de trabalho, em relação a papéis e mídias de armazenamento removíveis expostos sobre a mesa. Ao terminar o trabalho ou quando o colaborador não estiver fisicamente em seu posto de trabalho, nenhum documento, relatório e/ou mídia, confidencial e/ou restrito, deverá ser deixado sobre sua mesa.

19.3 Os documentos com informações sensíveis ou críticas, em papel ou em mídia de armazenamento eletrônicas, devem ser guardados em lugar seguro.

19.4 A política de “Tela Protegida” é aplicada à sessão e ao ambiente de trabalho do colaborador em seu computador/notebook, evitando, por exemplo, que sua sessão de trabalho autenticada/registrada permaneça aberta quando estiver ausente de seu ambiente de trabalho.

19.5 Quando o computador permanecer sem uso pelo período de 5 minutos, o sistema irá bloquear a tela automaticamente.

19.6 A política de Mesa Limpa e Tela Protegida resguarda ao INPAS, bem como o próprio colaborador, contra o acesso não autorizado a informações, evitando a visualização de informações expostas sobre a mesa ou na tela do computador.

20. Política de Impressão

20.1 O serviço de Impressão destina-se exclusivamente a atividades de cunho institucional.

20.2 Documentos que contenham informação classificada como confidencial ou restrita, nos termos da Cláusula 6 desta

Política, bem como dados de usuários de serviços do INPAS, devem ser removidos da impressora imediatamente.

20.3 O colaborador deve imprimir somente documentos relacionados às suas atividades institucionais.

20.4 A sustentabilidade ambiental é elemento chave na utilização do serviço, a impressão de documentos e deve ser evitada sempre que possível;

a) Deve-se sempre que possível usar impressão em face dupla.
b) Deve-se buscar a tramitação de documentos de forma eletrônica.

21. Backup de Dados e Cópias

21.1 Todos os dados deverão ser protegidos através de rotinas de "backup". Cópias de segurança dos sistemas serão executadas de forma automática, sendo o processo acompanhado pela unidade organizacional responsável pela Tecnologia da Informação.

21.2 É de responsabilidade dos usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos usuários, que não sejam considerados importantes às atividades da organização.

21.3 No caso das informações consideradas importantes às atividades da organização, o usuário tem obrigação de salvá-las na pasta de rede da sua área. Estas informações serão incluídas na rotina diária de "backup" automático.

21.4 Não é permitida a cópia, reprodução ou transferência (para e-mail pessoal ou transferência digital ou física a terceiros) de informações a que os usuários tenham acesso em decorrência do exercício de suas atividades, exceto quando previamente autorizado pelo titular da unidade organizacional. A não observância dessa regra caracteriza a quebra da obrigação de confidencialidade a que o usuário está comprometido em razão de sua função na organização, podendo acarretar sua responsabilização civil ou criminal, conforme o caso.

22. Política de Software

Hoje temos várias opções de softwares que podem ser utilizados para uma mesma finalidade, temos os softwares com licenças pagas e aqueles que utilizamos de forma gratuita. A prática do uso de software pirata ou conteúdo não legalizado, é um crime previsto na Lei nº 9.609/1998 que protege a propriedade intelectual no Brasil e prevê multa de até 10 vezes o valor original do software. Há ainda outros processos administrativos e judiciais que podem ser movidos contra o usuário do software e conteúdo não legalizado. A Lei Geral de Proteção de Dados (LGPD) - nº 13.709/2018, também prevê penalizações.

Com isso, cada secretaria/setor é responsável por realizar levantamento de necessidade do software desejado e planejar a sua aquisição, remetendo à Secretaria de Tecnologia da Informação e Proteção de Dados para fim de verificação de compatibilidade com o sistema operacional utilizado.

Revisões

Este documento foi revisado em maio de 2023 pelos colaboradores da Secretaria de Tecnologia da Informação e Proteção de Dados:

Flávio Holanda

Chefe de Tecnologia da Informação

Nerthan Buarque

Técnico de Processamento de Dados