



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Instituto Nacional de Proteção de Dados – INPD

Emissão: 31/07/2023

Classificação: Público

Versão: 2.0

Presidente: Rafael Reis

Vice-Presidente: Leandro Cruz

Comissão de Governança e Compliance

Coordenação

Atilio Augusto Segantin Braga

Membros

Daiane Dantas


Alessandra Mendonça

Guilherme Gonçalves

Janaína Lima


Roberta Gomes

i N P D
INSTITUTO NACIONAL DE
PROTEÇÃO DE DADOS

 INPD <small>INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS</small>	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis
Código PSI-001			

Sumário

1.	Introdução	2
2.	Propósito	3
3.	Objetivos	3
3.1.	Documentos de Referência	4
3.2.	Glossário	4
4.	Controles de Segurança da Informação	5
4.1.	Geração de Senhas	5
4.2.	Classificação da Informação	5
5.	Papéis e Responsabilidades	6
5.1.	Comitê de Privacidade	6
5.1.1.	Responsabilidade do Comitê de Privacidade:	7
5.1.2.	Gestores da Informação	7
5.2.	Usuários da Informação	8
5.3.	Dos Associados	8
6.	Salvaguarda de Registros do Instituto	9
7.	Identificação e Autenticação	10
8.	Autorização de Acesso	10
9.	Violação de dados pessoais	10
10.	Administração de Segurança	11
10.1.	Incidentes de Segurança	11
10.1.1.	O que fazer em caso de um incidente de segurança com dados pessoais?	12
11.	Backup e Recuperação	12
12.	Correio Eletrônico	13
13.	Controle de Versões	13
14.	Contato com autoridades	14
15.	Revisões	14
16.	Gestão da Política	14
17.	Aprovação	14

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS - INPD

Política de Segurança da Informação

1. Introdução

O Instituto Nacional de Proteção de Dados – INPD é uma organização civil sem fins lucrativos que visa fomentar a pesquisa, o debate, auxiliar a correta proteção de dados pessoais e viabilizar o diálogo entre titulares, empresas e Poder Público.


A Política de Segurança apresentada neste documento é de leitura mandatória por todos os associados, associados e fellows da instituição (por ex.: diretores, gestores, associados, terceiros entre outros) e deve ser entendido e usado como necessário para realizar seus deveres e atribuições.

Visando preservar a segurança e proteção dos dados, esta Política de Segurança da Informação define um conjunto de políticas com o propósito de garantir que todos os usuários do INPD conheçam as regras e diretrizes deste documento.

Também, manter o compromisso dos cuidados necessários com os dados pessoais de terceiros ao qual fazem parte da operação diária de nossas atividades, cumprindo as recomendações desta Política de Privacidade Interna, da Política de Segurança da Informação e das recomendações enviadas pelo Comitê de Privacidade do INPD.

A partir desse documento, o INPD formaliza seu comprometimento com o cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Por isso é fundamental que esta política seja disseminada entre todos os associados e colaboradores, pois sua observação e cumprimento será exigida em todos os níveis da organização sob pena das sanções aplicáveis

Nesta política os objetivos globais de Segurança da Informação do INPD são definidos através de um conjunto de normas de segurança, e deve ser vista como uma referência a todas as decisões relacionadas à Segurança da Informação

	<p align="center">POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</p>	<p align="center">Emissão 31/07/2023</p>	<p align="center">Classificação Interno</p>
<p align="center">Código PSI-001</p>		<p align="center">Versão 2.0</p>	<p align="center">Aprovado por: Rafael Reis</p>

2. Propósito

Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitem adotar padrões de comportamento seguro, adequados às metas e necessidades do INPD;

- a) Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
- b) Resguardar as informações do INPD, garantindo requisitos básicos de autenticidade, confidencialidade, integridade e disponibilidade;
- c) Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus associados, clientes e parceiros;
- d) Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio do INPD como resultado de falhas de segurança.

3. Objetivos

A Política de Segurança da Informação (PSI) do INPD tem como objetivo estabelecer as orientações, normas, ações e responsabilidades relativas à proteção da informação custodiada ou de propriedade do instituto.


Preservar e proteger as informações de nossos associados, funcionários, prestadores de serviços, partes interessadas e do próprio instituto contra ameaças e riscos relacionados à segurança da informação e segurança cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade do INPD a incidentes, e dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Temos ainda como objetivo preservar as informações quanto à:



- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **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.

- **Autenticidade:** garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação.


 INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis
Código PSI-001			

3.1. Documentos de Referência

- Política de Privacidade Externa
- Política de Privacidade Interna
- Política de Gestão de Incidentes

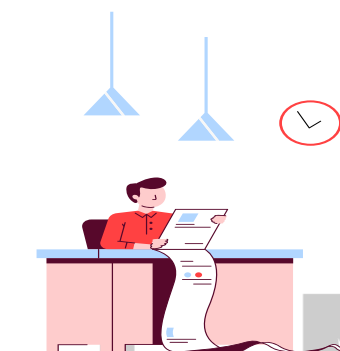
3.2. Glossário

Ameaça:	Causa potencial de um incidente, que pode vir a prejudicar o INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS;
Ativo:	Tudo aquilo que possui valor para O INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS;
Ativo de informação:	Patrimônio intangível do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas o INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do INPD ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.
Comitê de Privacidade e Segurança da Informação	Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do INPD, que tem por finalidade tratar questões ligadas à Segurança da Informação.
Confidencialidade e:	Propriedade dos ativos da informação do INPD, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.
Controle:	Medida de segurança adotada pelo INPD para o tratamento de um risco específico.
Disponibilidade:	Propriedade dos ativos da informação do INPD, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.
Gestor da Informação:	Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.
Governança de TI:	conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam a assegurar que as decisões e ações relativas à gestão e ao uso da TI mantenham-se alinhadas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais; Governança de TI: conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam a assegurar que as decisões e ações relativas à gestão e ao uso da TI mantenham-se alinhadas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais;
Incidente de segurança da informação:	Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS.
Integridade:	Propriedade dos ativos da informação do INPD, de serem exatos e completos.
Partes Interessadas:	indivíduos, unidades ou organizações que estejam diretamente envolvidos na gestão e na implementação da solução de TI, ou que, ainda que de forma indireta, possam exercer influência ou ser afetados pela solução;
Risco de segurança da informação:	Efeito da incerteza sobre os objetivos de segurança da informação do INPD.
Segurança da informação:	A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS.
Usuário da informação:	Diretores, Associados, Fellows ou terceiros alocados na prestação de serviços com o INPD, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS para o desempenho de suas atividades profissionais no âmbito de suas atividades.

 Código PSI-001	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis

Tecnologia da Informação e Comunicação (TIC):	conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios.
Vulnerabilidade:	Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS.
Tecnologia da Informação e Comunicação (TIC):	conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios.

4. Controles de Segurança da Informação



Os controles de segurança consistem em um conjunto amplo de medidas de segurança, compreendendo práticas de segurança comuns, e são necessários para implementar a PSI do INPD. Os controles de segurança são baseados na norma de segurança aceita internacionalmente (ISO 27001, ISO 27002, entre demais referências normativas e boas práticas de mercado).

A fim de assegurar que todas as diretrizes estabelecidas nesta política sejam cumpridas e que os princípios de Segurança da Informação e da Segurança Cibernética sejam devidamente seguidos, o INPD adotará procedimentos para os processos a seguir:

4.1. Geração de Senhas


Como prevenção de acesso indevidos:

- Todas as senhas devem ter ao menos 12 caracteres/
- Utilize a combinação de ao menos 5 palavras aleatórias, letras maiúsculas, números e símbolos;
- Evite criar senhas previsíveis;
- Senhas não podem ser reutilizadas; e
- As senhas não podem conter ou serem idênticas ao nome do usuário.

4.2. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o INPD e seus associados. Portanto, deve adotar a seguinte classificação:

- ❖ **Informação Pública:** aquela que pode ser acessada por todos, sem restrição. São exemplos: material didático elaborado pelo instituto, guias criados com a finalidade de contribuir com o amadurecimento

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

do ecossistema, eventos públicos, divulgação de artigos técnicos e orientações de um modo geral destinadas ao público externo.

- ❖ **Informação Interna:** aquela que pode ser acessada somente por funcionários, membros da direção e associados. São exemplos: Normas, procedimentos, formulários instruções internas.
- ❖ **Informação Restrita:** aquela que pode ser acessada somente por funcionários e membros de comissão que precisam dela para desempenhar suas atribuições. São exemplos: contratos e documentos estratégicos do INPD; e
- ❖ **Informação Confidencial:** aquela que pode ser acessada somente por colaboradores e membros da direção que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos: plano estratégico e informações pessoais dos associados.

5. Papéis e Responsabilidades




Serão responsabilizados pelos seus atos e omissões não aderentes a esta política aqueles que criarem, modificarem, armazenarem e transmitirem qualquer informação pertencente ao INPD, sejam estes associados, fellows, diretores, membros de comissões, terceiros ou parceiros, cuja sanção e/ou advertência ou até mesmo exclusão será avaliada e imposta pelo Comitê descrito no item 5.1 desta política.

A utilização inadequada da informação pode resultar em responsabilização previstas no Estatuto, Políticas e Procedimentos internos, além de penalidades previstas por lei.

5.1. Comitê de Privacidade



O Comitê de Privacidade é responsável pela aprovação das normas, políticas de procedimentos, bem como eventuais sanções a serem aplicadas.

 INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis
Código PSI-001			

5.1.1. Responsabilidade do Comitê de Privacidade:

- i. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
- ii. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- iii. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PSI;
- iv. Decidir qualquer assunto relevante relacionado ao cumprimento da presente Política de Segurança da Informação, bem como que coloque em risco aspectos reputacionais do INPD.
- v. Compete ao Comitê decidir sobre aspectos que possam comprometer o Sistema de Gestão da Informação e Privacidade do INPD.

5.1.2. Gestores da Informação

É responsabilidade de todos os membros do instituto que executem atividades inerentes a gestão da informação. Como por exemplo: Secretaria Geral, Presidente de Comissões, Secretários, Membros de Comissões, Diretor Financeiro, Vice-Presidente e Presidente:

5.2.1. Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo INPD;

5.2.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo INPD;

5.2.3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;


5.2.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.2.5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo INPD.

5.2.6. Manter atualizado o Registro das Atividades de Tratamento que realizarem.

5.2.7. Levar em consideração o *Privacy by design* na avaliação de toda e qualquer nova atividade de tratamento de dados do Instituto.

5.2.8. Comunicar o Encarregado de Dados e/ou Comitê de Governança e Compliance – CGC da intenção de implementar uma nova atividade de tratamento de dados pessoais, levando a privacidade como premissa da atividade e somente realizá-la após ciência do registro de sua atividade no Registro de Atividades de Tratamento.

 INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis
Código PSI-001			

5.2. Usuários da Informação

É RESPONSABILIDADE DOS USUÁRIOS DA INFORMAÇÃO:	
Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;	Assinar o Termo de Uso de Sistemas de Informação do INPD, formalizando a ciência e o aceite das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, a Comissão de Governança e Compliance;	Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.
Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do INPD;	


5.3. Dos Associados

O(A) Associado(a) deverá adotar medidas de segurança nos aplicativos de mensageria, recomendando, no mínimo as seguintes medidas:

- Manter a ferramenta sempre atualizada;
- Ativar a confirmação em duas etapas e forneça um endereço de -e-mail para que possa redefinir seu PIN caso o esqueça;
- Bloquear o acesso do aplicativo mediante senha forte;
- Exibir sua foto somente para seus contatos;
- Evitar utilizar conexões compartilhadas;
- Nunca compartilhar seu código de confirmação e seu PIN da confirmação em duas etapas;
- Proteja sua caixa postal com uma senha forte;
- Confira com frequência os aparelhos que estão conectados à sua conta;
- Defina uma senha para seu aparelho e atente-se a quem tem acesso físico ao seu celular.

Pessoas com acesso físico ao dispositivo podem usar sua conta sem sua permissão.

Revise com frequência as configurações de privacidade do seu celular e dos aplicativos de mensageria. Tal medida é importante pois um dos canais de comunicação

 INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

com o INPD é o Whatsapp que poderá conter dados pessoais dos (as) associados(as) do instituto.

O Instituto Nacional de Proteção de Dados Pessoais não coleta dados sensíveis, todavia, em algumas situações é possível que um (a) associado(a) compartilhe a data de seu aniversário em nossos canais. Caso ocorra esse tipo de compartilhamento iremos conservar essa informação para manutenção do histórico de comunicação em nossos canais de mensageria.

Caso o associado(a) não deseje mais integrar o INPD seus dados serão conservados para fins de cumprimento de obrigação legal e conservados de acordo com o legítimo interesse do instituto em manter seus registros.

Nos grupos de comunicação e de trabalho do instituto as mensagens devem se limitar:

- Assuntos para o qual o grupo foi criado
- Assuntos Políticos, religiosos, futebolísticos e outros que não estejam relacionados à segurança da informação e proteção de dados, controles internos e governança de dados só devem ser tratados no privado, NUNCA em grupo;
- Correntes, campanhas e boatos de internet não interessam aos grupos profissionais do INPD, salvo para efeito de estudo de casos;
- Arquivos contendo fotos, vídeos devem estar relacionado ao tema para o qual o grupo foi criado.


6. Salvaguarda de Registros do Instituto



O(A) Associado(a) deverá adotar medidas de segurança nos aplicativos de mensageria, recomendando, no mínimo as seguintes medidas:

Registros importantes do instituto devem ser protegidos contra perda, destruição e falsificação. Alguns registros podem necessitar de retenção segura para atender a requisitos estatutários ou regulamentares, bem como apoiar atividades essenciais.

O sistema de armazenagem e manuseio de registros deve assegurar a clara identificação de registros e de seu período de retenção estatutário ou regulamentar. Deve permitir a destruição apropriada dos registros após esse período se o INPD não mais necessitar deles.

 INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
		Versão 2.0	Aprovado por: Rafael Reis
Código PSI-001			

7. Identificação e Autenticação

A autenticação de usuários do INPD é efetuada mediante senha; os usuários devem manter a sua senha em segredo, modificá-la regularmente, não devem armazená-las em seus computadores, e não devem tentar descobrir senhas pertencentes a outras pessoas. Devido à responsabilidade pessoal, o uso de credenciais de acesso funcionais ou compartilhadas não é permitido. Exceções podem ser concedidas desde que procedimentos adequados para o acesso controlado às credenciais de acesso funcionais ou compartilhados sejam aplicados.



É recomendável que medidas adicionais e mais fortes de identificação e autorização sejam implementadas para usuários e parceiros do INPD quando necessário. Para um perfil com privilégios especiais, é recomendável considerar o uso de técnicas mais rígidas de autenticação, tais como tokens ou pergunta/resposta.

8. Autorização de Acesso

Controle de acesso é exigido para sistemas e dados compartilhados com outros. O proprietário da informação em um sistema compartilhado é responsável por decidir quem poderá acessar e que autoridades serão concedidas.




9. Violação de dados pessoais

A violação de dados pessoais ocorre quando o INPD sofre um incidente de segurança relativo aos dados pessoais pelos quais são responsáveis e que resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados.



Em outras palavras, um incidente de segurança com dados pessoais pode ser qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

 <small>INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS</small>	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

Se essa violação for suscetível de representar um risco para os direitos e as liberdades de uma pessoa o INPD tem de notificar a autoridade de controle sem demora injustificada. Assim, caso qualquer colaborador interno, parceiro comercial, fornecedor de produtos ou serviços ou qualquer cidadão tomar conhecimento da possibilidade de ocorrência de um vazamento de dados pessoais ou de incidente de segurança deve imediatamente comunicar o setor de privacidade e o Encarregado de Dados através do e-mail dpo@inpd.com.br.

No caso de ter sido identificada uma violação de dados pessoais, e após avaliação de impacto, caso seja identificado que o vazamento implica em um elevado risco para os direitos e liberdades do titular dos dados afetados, o INPD compromete-se a efetuar a comunicação no prazo de até 3 dias da violação de dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados a contar do conhecimento do incidente, salvo estabelecimento de um prazo menor pela agência reguladora.

A comunicação ao titular dos dados não será efetuada nas seguintes situações:

- No caso de terem sido aplicadas todas as medidas de proteção adequadas aos dados pessoais em causa, tanto técnicas como organizativas, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a acessar esses dados, tais como a encriptação ou anonimização;
- No caso de terem sido tomadas medidas subsequentes que assegurem que deixou de haver risco para os titulares dos dados em causa; ou
- No caso da comunicação aos titulares dos dados implique um esforço desproporcional. E neste caso poderá ser efetuada uma comunicação pública ou algo semelhante que possa permitir que os titulares dos dados sejam informados.


10. Administração de Segurança

É recomendável haver um procedimento de registro de usuário para entrada de novos usuários em um sistema. Somente pedidos aprovados pelo proprietário da informação em um sistema, podem ser implementados. Um registro de todos os usuários registrados para usar o sistema deve estar disponível.



É recomendável existir um processo estabelecido para bloquear ou excluir credenciais de acesso mediante notificação.

10.1. Incidentes de Segurança

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

Incidentes de segurança não podem ser publicados e devem ser notificados imediatamente para o dpo@inpd.com.br.



Ao tomar ciência do incidente fica sob a responsabilidade do DPO conduzir o tema juntamente com o Comitê de Privacidade, que deverá elaborar plano de ação para correção da falha ou mitigar danos.

A gestão sobre ameaça deve seguir os seguintes passos:

1. Observação: validar e garantir que a ameaça existe.
2. Orientação: checar histórico de ameaças e analisar impactos da ameaça.
3. Decisão: elaboração do plano de ação.
4. Ação: Criação do comitê para elaborar a correção e testar se a falha foi corrigida.

10.1.1. O que fazer em caso de um incidente de segurança com dados pessoais?

Inicialmente qualquer suspeita de um incidente ou possibilidade de incidente deve ser comunicada ao Encarregado de Dados através do e-mail dpo@inpd.com.br

A avaliação interna do incidente será realizada de acordo com a política de gestão de incidentes, pelo setor de processos e privacidade em conjunto com o Encarregado de dados e conforme o caso, levado ao conhecimento do Comitê de Privacidade, sendo certo que terão a responsabilidade de avaliar a: natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis.

Diante da avaliação do Comitê será realizado comunicado à Autoridade Nacional de Proteção de Dados – ANPD e conforme o caso, aos titulares de dados, em caso de risco ou dano relevante aos titulares, nos termos do artigo 48 da LGPD.


Caso o INPD atue como Operador de dados o Encarregado fará a comunicação ao Controlador, informando as medidas que estão sendo adotadas.

11. Backup e Recuperação

Instalações adequadas de backup, de acordo com a importância e valor do sistema e dos dados, devem ser fornecidas para assegurar que software de sistemas, software de aplicativo e dados possam ser recuperados após uma falha de mídia ou de sistema.



É recomendável que arquivos de backup sejam armazenados em local remoto, a distância suficiente do local principal e, providos com o nível adequado de proteção

 <small>INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS</small>	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

física, consistente com a segurança física do local principal. É recomendável que o processo de backup e restauração seja testado regularmente.

12. Correio Eletrônico

É recomendável que os membros do INPD estejam cientes de que mensagens eletrônicas podem ser encaminhadas, interceptadas, impressas e armazenadas por outras pessoas. A menos que a mensagem seja criptografada, os usuários devem evitar enviar informações sensíveis via e-mail.

O emissor de uma mensagem eletrônica é considerado pessoalmente responsável por seu conteúdo. É recomendável que os associados estejam cientes de que todas as mensagens originadas levam o nome do INPD em seu endereço de origem.

É recomendável que toda mensagem seja preparada e enviada de maneira profissional seguindo todas as regras de decoro social. Da mesma forma, os associados do INPD devem evitar enviar mensagens que podem ser consideradas inflamatórias, discriminatórias, injuriosas ou de outra forma ofensivas ou ilegais.

É recomendável que os associados do INPD exerçam com cuidado o encaminhamento de mensagens, reconhecendo que certas informações são dirigidas a indivíduos específicos e podem não ser adequadas para distribuição geral em comunicações eletrônicas.

E-mails indesejados ou "spam" são considerados ofensivos e e-mail contendo material ilegal, ofensivo ou malicioso é considerado intolerável.

É recomendável que ao visitar websites e tendo que preencher informações, os associados tomem cuidado antes de usar o endereço de e-mail do INPD. Isto pode resultar em e-mail comercial indesejado e não solicitado.


É recomendável que os associados evitem deixar seus endereços de e-mail do INPD se a política de privacidade do website é inexistente ou declarar que aquela informação será vendida ou compartilhada.

13. Controle de Versões



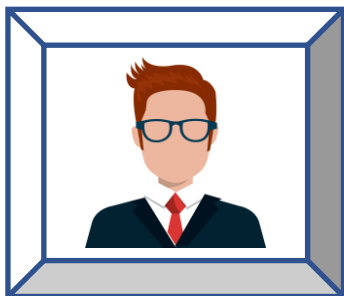
O INPD respeitará a privacidade de seus usuários de e-mail. Normalmente usuários de e-mail podem presumir que somente o destinatário lê sua correspondência eletrônica.

Entretanto, o acesso a caixas de correio eletrônico de usuários pode ser solicitado no caso de qualquer urgência, incluindo atividades de investigação. Também pode ser necessário para o suporte técnico revisar o conteúdo das

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

comunicações de membros individuais dos associados durante a resolução de problemas.

14. Contato com autoridades



Objetivo: Especificar quando, por quem e quais autoridades (por exemplo, obrigações legais, polícia, corpo de bombeiros, autoridades fiscalizadoras, organismos regulatórios) serão contatadas e como os incidentes de segurança da informação identificados serão reportados em tempo hábil.

- O INPD, com o apoio do Comitê descrito no item 5.1, desta política, deve especificar quais as autoridades são essenciais para apoiar a segurança da informação.
- O INPD deve definir quem são as pessoas que podem ter contato com as autoridades em nome da organização.
- O INPD deve disponibilizar em local de fácil acesso e visualização, as autoridades e os meios de contato.
- Cabe somente ao Encarregado manter e receber comunicações da ANPD e adotar providências e/ou pessoa designada para exercício de suas atividades.

15. Revisões


Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê de Privacidade.

16. Gestão da Política

A Política Geral de Segurança da Informação é aprovada pelo Comitê de Privacidade, em conjunto com a Diretoria do INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS.

17. Aprovação

A presente política foi revisada e aprovada no dia 30/07/2023.

 <small>INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS</small>	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 31/07/2023	Classificação Interno
Código PSI-001		Versão 2.0	Aprovado por: Rafael Reis

Para firmeza e como prova de assim haverem aprovado, a alta direção do INPD assina física e/ou digitalmente. Conforme previsto no Art. 107 do Código Civil, Medida Provisória nº 2.200-2/2001, Art. 10, § 2, Enunciado 297 do Conselho da Justiça Federal.

Presidente

Presidente da Comissão de Governança e Compliance

Vice-Presidente da Comissão de Governança e Compliance

