# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SEROPÉDICA/RJ, 27 de março de 2025.

Versão 3.0

Aprovado na 69ª Reunião Ordinária do Conselho de Administração

Histórico de versões

| DATA | VERSÃO | DESCRIÇÃO | AUTOR |
|---|---|---|---|
| 19/04/2022 | 1.0 | Versão inicial | Gabinete do Diretor-Presidente |
| 22/12/2023 | 2.0 | Adequação à LGPD | Gabinete do Diretor-Presidente |
| 25/03/2025 | 3.0 | Ampliação da abrangência da Política | Setor de Tecnologia da Informação |

## 1. DA APRESENTAÇÃO

1.1 A Política de Segurança da Informação objetiva orientar e estabelecer as diretrizes administrativas para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas do Instituto e por todos os servidores, estagiários, membros de órgãos colegiados e prestadores de serviço que tenham acesso às informações de propriedade do Seroprevi e aos dados pessoais de titulares tratados pelo Instituto.

1.2 É um dos instrumentos primordiais na constituição do Programa de Governança em Privacidade e Proteção de Dados Pessoais na forma do inciso I, § 2º, art. 50 da Lei Federal nº 13.709 de 2018 - Lei Geral de Proteção de Dados Pessoais.

1.3 O Instituto adota como princípio a tolerância zero a qualquer tipo de fraude ou corrupção, condenando veementemente suas práticas, de modo que o uso das informações do Instituto e dos dados pessoais sob sua guarda para fins diversos daqueles exigidos será severamente punido.

1.4 Sabemos o quanto a corrupção está arraigada na cultura patrimonialista que forjou a sociedade brasileira. Por isso, é preciso que todos se mantenham sempre vigilantes e atentos aos limites entre o público e o privado, para que seja garantida total segurança as informações pertencentes ao Instituto.

1.5 Da mesma forma, a Lei Geral de Proteção de Dados Pessoais inovou ao garantir direitos aos titulares dos dados e obrigações ao Poder Público no curso do tratamento desses dados, estabelecendo sanções que podem ser aplicadas pelo descumprimento da lei.

## 2. DOS OBJETIVOS

A Política de Segurança da Informação objetiva normatizar os procedimentos relativos a segurança da informação no âmbito do Instituto, além de garantir a integridade e a segurança das informações dentro dos mais elevados padrões de governança corporativa, objetivando assegurar:

a) diretrizes que permitam aos servidores, estagiários, membros de órgãos colegiados e fornecedores do Instituto seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do titular dos dados pessoais;

b) nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento; e

c) preservar as informações do Instituto e os dados pessoais dos titulares quanto à integridade, confidencialidade e disponibilidade.

3. DOS PRINCIPIOS

São princípios da Política de Segurança da Informação:

a) A confidencialidade, que consiste na proteção e na garantia de que as informações só são acessíveis a pessoas autorizadas;

b) A integridade que garante a exatidão das informações e dos métodos de processamento, evitando adulterações e fraudes; e

c) A disponibilidade, imprescindível para que os usuários autorizados e os interessados tenham acesso às informações em tempo real ou sempre que solicitado.

4. DA ABRANGÊNCIA

A Política de Segurança da Informação abrange todos os agentes políticos, servidores, estagiários, conselheiros, membros de colegiados, parceiros e prestadores de serviço que tenham acesso a informações do Instituto.

5. DAS RESPONSABILIDADES

5.1 É responsabilidade dos servidores, estagiários, membros de órgãos colegiados e fornecedores do Instituto:

a) Manter sigilo das informações;

b) Zelar continuamente pela proteção das informações contra acesso, modificação, destruição ou divulgação não autorizada;

c) Assegurar que os recursos tecnológicos colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;

d) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

e) Comunicar imediatamente ao Setor de Tecnologia da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação;

f) Seguir as diretrizes e recomendações quanto ao uso, divulgação e descarte de dados e informações; e

g) Cumprir e fazer cumprir esta política, as normas e procedimentos de segurança da informação.

5.2 É de responsabilidade das chefias dos setores do Instituto:

a) Classificar a informação sob sua responsabilidade;

b) Inventariar toda a informação sob sua responsabilidade;

c) Sugerir procedimentos para proteger a informação sob sua responsabilidade;

d) Manter um controle efetivo do acesso à informação em seu setor;

e) Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

f) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade;

g) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

h) Sugerir ao Setor de Tecnologia da Informação, de maneira proativa, procedimentos de segurança da informação relacionados ao seu setor;

i) Comunicar imediatamente ao Setor de Tecnologia da Informação eventuais casos de violação desta política, de normas ou de procedimentos de segurança da informação.

6. DO USO DA INTERNET

6.1 O acesso à Internet será autorizado para servidores, estagiários, membros de órgãos colegiados e fornecedores do Instituto desde que atendam as regras desta Política de Segurança da Informação e das demais normas de segurança da informação.

6.2 O acesso à Internet será autorizado a visitantes somente através de wi-fi, desde que devidamente identificados através de registro de acesso.

6.3 A internet poderá ser utilizada para fins pessoais, desde que não prejudique o andamento das atividades ou causem prejuízo ao instituto.

6.4 Todo acesso à internet será identificado através da conta e senha do usuário, com o ambiente monitorado.

6.5 O acesso à internet se caracteriza como uma ferramenta de trabalho, sendo seu uso destinado às funções relativas as atribuições funcionais.

6.6 Será permitido o acesso à internet para uso com fins particulares nas seguintes condições, cumulativamente:

a) seja utilizado para acesso à Internet Bank e a sites cujo conteúdo proporcionem desenvolvimento pessoal;

b) o tempo de acesso e conteúdo acessado não interfiram no cumprimento dos deveres;

c) o acesso não interfira no bom funcionamento da rede e dos sistemas do Instituto;

d) não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;

e) todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado; e

f) o acesso não coloque em risco a segurança da rede e dos sistemas do instituto.

6.7 Em caso de sobrecarga da rede e/ou lentidão da internet, serão priorizados os acessos para fins funcionais, devendo os acessos para fins particulares serem interrompidos até normalização da rede.

6.8 O acesso à internet poderá ser bloqueado a qualquer momento por decisão do Setor de Tecnologia da Informação ou do Gabinete do Diretor-Presidente.

7. DO USO DO E-MAIL INSTITUCIONAL

O servidor ou estagiário receberá, obrigatoriamente, correio eletrônico funcional para fins de serviço, e acesso ao correio eletrônico setorial, sendo terminantemente proibido:

a) enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao exercício de suas funções;

b) acessar o correio eletrônico de outro usuário sem a devida autorização;

c) enviar mensagem pelo seu correio fazendo-se passar por terceiro;

d) enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Instituto vulneráveis a ações civis ou criminais;

e) divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

f) falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas na legislação em vigor; e

g) apagar mensagens pertinentes de correio eletrônico quando o Instituto estiver sujeito a algum tipo de investigação.

8. DO USO CONSCIENTE DA INTERNET E DO E-MAIL

O usuário da internet e do e-mail deverá estar ciente de que:

a) deve ter comportamento ético e profissional com o uso da internet e intranet disponibilizada pela rede cabeada e pelo serviço de wi-fi;

b) qualquer informação acessada, transmitida, recebida ou produzida na internet ou intranet estará sujeita a divulgação e auditoria, tendo o Instituto, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela;

c) o uso de qualquer recurso do Instituto para atividades ilícitas acarretará as devidas sanções administrativas, sendo que o Instituto cooperará ativamente com as autoridades competentes afim de se esclarecer as ilegalidades cometidas;

d) as ações deverão sempre pautar-se pelos princípios dispostos na Lei de Direitos Autorais, na Lei Geral de Proteção de Dados, e na proteção a imagem garantida pela Constituição Federal; e

e) deverá zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

9. DO USO DOS COMPUTADORES E OUTROS EQUIPAMENTOS TECNOLÓGICOS

9.1 Todos os equipamentos pertencentes ao Instituto são de uso exclusivo para as atividades administrativas e são disponibilizados de acordo com as necessidades e especificidades dos setores e dos usuários para o desempenho de suas funções.

9.2 Os usuários são responsáveis pelos equipamentos disponibilizados, devendo assinar o Termo de Disponibilização quando do primeiro acesso ao equipamento pessoal, sendo responsabilizados caso haja caracterização de mau uso, e assinarem o Termo de Cessão da Disponibilização quando do término do uso do equipamento.

9.3 O equipamento disponibilizado não poderá ser utilizado em atividades externas e/ou retirado da sede do Instituto, salvo com autorização expressa por escrito do Gabinete do Diretor-Presidente.

9.4 Em caso de perda ou subtração de equipamento, o servidor deverá comunicar imediatamente sua chefia e o Gabinete do Diretor-Presidente, apresentando relatório por escrito dos fatos ocorridos em até 24 horas após a ciência destes.

9.5 O mau uso será caracterizado quando houver reconhecimento por parte do usuário ou por decisão técnica do Analista de Sistemas com anuência da Diretoria-Executiva.

9.6 E vedada a inserção de pen-drives, CD's, cartões de memória ou a conexão de qualquer outro dispositivo nos equipamentos, inclusive celulares, mesmo que somente para carga.

9.7 Somente poderão ser acessados e compartilhados arquivos em drives oficiais do Instituto, podendo cada setor possuir sua conta específica, sendo vedado o compartilhamento de arquivos em drives pessoais e de terceiros.

9.8 Em caso de troca de usuário do equipamento, todos os arquivos deverão ser retirados pelo usuário de saída, e o equipamento deverá ser formatado para uso do novo usuário.

9.9 As senhas deverão ser trocadas periodicamente, devendo expirar após três meses de uso, sendo vedado o uso de senha anterior, data de aniversário e números sequenciais, e obrigatório que contenha caracteres especiais, números, letras maiúsculas e minúsculas.

9.10 As senhas deverão ser gravadas pelos usuários, sendo vedado seu registro ou salvamento no equipamento ou em papel a ser armazenado nas instalações do Instituto, e vedado expressamente o salvamento das senhas.

9.11 É vedado o compartilhamento de logins, senhas e equipamentos, salvo por autorização expressa por escrito do Gabinete do Diretor-Presidente, sendo proibido ao usuário o uso de equipamentos de terceiro.

10. DO USO DOS NOTEBOOKS E CELULARES FUNCIONAIS

10.1 O Diretor-Presidente, o Diretor Administrativo e Financeiro, e o Subgerente de Tesouraria farão jus a disponibilização por parte do Instituto de notebook e celular para uso funcional devido ao acesso as contas bancárias do Instituto.

10.2 Ao receber ou devolver o notebook e o celular funcional o servidor deverá assinar termo de recebimento ou devolução do equipamento.

10.3 O servidor que estiver de posse de notebook ou celular funcional tem o dever de zelar pela guarda do equipamento, sendo de sua responsabilidade o ressarcimento ao Instituto por qualquer dano causado ao equipamento.

10.4 É vedado o uso do notebook ou celular funcional para fins pessoais diversos daqueles relacionados ao exercício da função do cargo que ocupa.

10.5 É vedado o acesso as contas bancárias do Instituto de notebook ou celular de uso pessoal, sendo permitido o acesso apenas por equipamentos pertencentes ao Instituto.

10.6 O servidor que estiver de posse de notebook ou celular funcional e for desligado do cargo em que ocupa tem o prazo máximo de 72 horas para realizar a devolução do equipamento sob pena de responsabilização civil e criminal.

10.7 Sempre que determinado, seja pelo Setor de Tecnologia da Informação ou pelo Gabinete do Diretor-Presidente, o servidor que estiver de posse de notebook ou celular funcional deverá apresentá-lo no prazo máximo de 72 horas sob pena de responsabilização administrativa.

11. DOS PROCEDIMENTOS DE CONTIGÊNCIA

11.1 O procedimento de contingência compreende a realização de backups (cópias de segurança) dos arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade, sendo responsabilidade do Setor de Tecnologia da Informação.

11.2 Para garantir a segurança da informação, são realizadas cópias de segurança dos arquivos mantidos em servidores, sistemas e respectivos bancos de dados utilizados pelo Instituto.

11.3 As rotinas de cópia de segurança são realizadas de forma automatizada, sob supervisão do Setor de Tecnologia da Informação, em horários pré-definidos, fora do horário de funcionamento do Instituto, denominadas de “Janelas de Backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processamento sendo realizado nos sistemas informatizados.

11.4 Mensalmente o Setor de Tecnologia da Informação realizará verificações dos backups realizados e testes de restauração com o intuito de averiguar a integridade dos arquivos ou banco de dados.

11.5 Quando identificado erro na cópia de segurança, seja na execução do backup e/ou no processo de restauração, é realizado um novo backup no primeiro horário disponível, após identificado e solucionado o problema.

11.6 O armazenamento das cópias de segurança é feito no Setor de Tecnologia da Informação, onde o acesso é controlado.

11.7 Os prestadores de serviço ao Instituto tem a obrigação de realizar as cópias de segurança e garantir a integridade do seu armazenamento para caso seja necessário realizar a restauração dos dados.

11.8 O Setor de Contratações deverá garantir o cumprimento do item 11.7 nos processos licitatórios em que envolva sistemas e/ou banco de dados.

11.9 As solicitações de restauração de arquivos deverão ser feitas formalmente ao Setor de Tecnologia da Informação.

11.10 É vedado o armazenamento de informações que estejam em desacordo com as atividades ou normas do Instituto, sob pena de responsabilização administrativa.

11.11 É vedado o compartilhamento ou extração de cópias de segurança sem prévia autorização do Gabinete do Diretor-Presidente, sob pena de responsabilização administrativa.

12. DO CONTROLE DE ACESSO FÍSICO E LÓGICO

12.1 A Sala do Servidor é uma instalação física centralizada onde está localizado o servidor, o sistema de câmeras de segurança e o sistema de alarmes, e onde funciona o Setor de Tecnologia da Informação.

12.2 O acesso a Sala do Servidor é restrito aqueles lotados no Setor de Tecnologia da Informação ou por autorização destes.

12.3 A Sala do Servidor será monitorada de forma intermitente com câmeras de segurança que registrem imagem e áudio.

12.4 O acesso a Sala do Servidor se dará através de fechadura com senha.

12.5 Somente o Setor de Tecnologia da Informação e o Gabinete do Diretor-Presidente terão a senha da fechadura de acesso a Sala do Servidor.

12.6 A Sala do Servidor será climatizada de forme intermitente, e em caso de inoperância dos aparelhos de ar-condicionado, o servidor deverá ser desligado para garantia de sua integridade.

12.7 Qualquer manutenção ou limpeza da Sala do Servidor só poderá ocorrer na presença de um servidor ou estagiário do Setor de Tecnologia da Informação.

12.8 É vedada a permanência na Sala do Servidor de terceiros sem a presença de um servidor ou estagiário do Setor de Tecnologia da Informação.

12.9 Não é permitida a entrada na Sala do Servidor de nenhum tipo de alimento, bebida, produto químico ou inflamável.

13. DO SETOR DE TECNOLOGIA DA INFORMAÇAO

13.1 O Setor de Tecnologia da Informação é responsável pela aplicação desta política e por sua revisão anual, bem como pela gestão da segurança da informação do Instituto.

13.2 Compete ao Setor de Tecnologia da Informação:

a) prover todas as informações de gestão de segurança da informação do Instituto;

b) prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços;

c) promover ações de conscientização sobre segurança da informação para os servidores e prestadores de serviços;

d) propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação; e

e) elaborar e manter política de classificação da informação, com temporalidade para guarda.

14. DA CLASSIFICAÇÃO DAS INFORMAÇÕES

A classificação das informações é parte do processo de gestão e análise das informações geradas pelo Instituto, competindo a chefia de cada setor a classificações das informações produzidas no seu setor, atendendo as seguintes classificações:

a) Pública: informação que pode ser acessada por qualquer pessoa, que não contenha dados pessoais ou informações sensíveis.

b) Restrita: informação que só pode ser acessada por servidores, estagiários, conselheiros e membros de colegiados do Instituto, e que contenha dados internos do Instituto, sendo que o acesso indevido deverá ser imediatamente comunicado pela chefia que o classificou ao Comitê de Ética Pública para apuração do acontecido.

c) Sigilosa: informação que só pode ser acessada mediante autorização do Gabinete do Diretor-Presidente, pois contem dados internos sensíveis a imagem do Instituto, sendo que o acesso indevido deverá ser imediatamente comunicado pela chefia que o classificou ao Gabinete do Diretor-Presidente para instauração de sindicância e apuração dos fatos.

15. DA TEMPORALIDADE E DA GUARDA DE DOCUMENTOS

| TEMPO DE GUARDA | TIPOS DE DOCUMENTOS |
|---|---|
| 5 anos | Cartão Corporativo<br>Contracheque<br>Documentos fiscais<br>Memorandos<br>Órgãos colegiados |
| 10 anos | Aplicações e resgates<br>Comitê de Investimentos<br>Ofícios<br>Registro de ponto |
| 20 anos | Atestado de Saúde Ocupacional (a contar do desligamento do servidor)<br>Auditoria externa<br>Auditoria interna<br>Investimento<br>Orçamento |

| TEMPO DE GUARDA | TIPOS DE DOCUMENTOS |
|---|---|
| 30 anos | Folha de pagamento<br>Fundo de Garantia por Tempo de Serviço - FGTS<br>Processo Administrativo Disciplinar<br>Sindicância |
| Indeterminado | Contrato<br>Contrato de trabalho<br>Convênio |

16. DA AUDITORIA

16.1 Todas as informações e procedimentos do Setor de Tecnologia da Informação serão passíveis de auditoria interna.

16.2 Anualmente a Controladoria Autárquica deverá realizar Auditoria Interna nos procedimentos do Setor de Tecnologia da Informação, que deverá fornecer todos os dados solicitados.

16.3 Semestralmente o Setor de Tecnologia da Informação deverá sortear cinco usuários para auditoria em seus acessos e equipamentos, sem aviso prévio, remetendo o relatório ao Gabinete do Diretor-Presidente.

16.4 Durante a execução de auditoria deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do Instituto.

16.5 Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, o Setor de Tecnologia da Informação poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas, desde que ao término o Gabinete do Diretor-Presidente seja devidamente comunicado.

16.6 As informações obtidas nas auditorias poderão servir como indício ou evidência em sindicância, processo administrativo ou processo judicial.

17. DOS RISCOS

17.1 São riscos típicos:

a) Vazamento, compartilhamento ou revelação de informações sensíveis ou dados pessoais;

b) Modificação indevida de dados e programas;

c) Perda de dados;

d) Destruição ou perda de dados, equipamentos e recursos tecnológicos;

e) Interdição ou interrupção dos serviços prestados;

f) Roubo ou furto dados;

g) Utilização indevida de dados; e

h) Acesso não autorizado a dados.

17.2. Os riscos são causados geralmente por:

a) Negligência - atos não intencionais de usuários;

b) Subversão - ataques disfarçados praticados por usuários;

c) Acidente - ocorrências acidentais e por fatores alheios;

d) Ataque furtivo - ataques praticados por pessoas estranhas;

e) Ataque forçado - ataques às claras praticados por usuários ou estranhos; e

f) Condutas ilícitas - ocorrências Ilícitas e por fatores alheios.

18. DAS AÇÕES DE MONITORAMENTO E SEGURANÇA

O Instituto poderá, afim de garantir a efetividade desta política:

a) implementar sistemas de monitoramento de equipamentos e usuários;

b) realizar auditorias nos sistemas e inspeções nos equipamentos, com emissão de relatórios periódicos;

c) instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e

d) estabelecer limites de acesso à intranet, acompanhando periodicamente os acessos e logins.

19. DA UTILIZAÇÃO ACEITÁVEL DA TECNOLOGIA

19.1 Como condição, as áreas que fazem usos dos recursos de tecnologia não poderão usá-los para quaisquer propósitos que sejam ilegais ou proibidos, tais como:

a) material sexualmente explícito;

b) material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;

c) apologia à violência ou ao terrorismo;

d) apologia às drogas;

e) violação de direito autoral (pirataria);

f) execução de quaisquer tipos ou formas de fraudes; e

g) compartilhamento de arquivos estranhos às atividades do Instituto e não autorizados pelo superior hierárquico.

19.2 Não é permitido ao usuário danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço, bens ou conteúdo, ou interferir no uso e participação de qualquer um dos usuários.

19.3 Não é permitido tentar obter acesso não autorizado a qualquer área, serviço ou conteúdo dos sistemas ou redes de computadores conectados, através de ações mal-intencionadas, corrupção de senha ou outros meios.

19.4 O uso e o acesso pelo usuário à rede corporativa, computadores, Internet e/ou utilização de e-mail corporativo, deverá ser exclusivo para uso profissional, para a execução e desempenho dos objetivos do Instituto, salvo por autorização expressa do superior hierárquico.

19.5 O Instituto reafirma que o uso da internet é uma ferramenta valiosa e importante para os trabalhos de seus colaboradores, mas o mau uso pode ter impacto negativo sobre a produtividade e a reputação, sendo dever de todos zelar pelo bom uso das ferramentas oferecidas.

19.6 E proibida a transferência de qualquer tipo de programa, jogo e similares para a rede interna sem autorização específica do superior hierárquico.

19.7 É proibido o uso de jogos, inclusive os da Internet (on-line).

19.8 É proibida a instalação de qualquer tipo de software, aplicativos ou jogos, salvo aqueles autorizados pelo Setor de Tecnologia da Informação.

20. DA FISCALIZAÇÃO E BOM USO DOS RECURSOS

O Setor de Tecnologia da Informação se reserva ao direto de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, esteja ele no disco local da estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na Rede com os endereços web (http://) visitados, visando assegurar o cumprimento desta política.

21. DAS SENHAS E ACESSOS

21.1 As senhas distribuídas para uso dos sistemas e acesso ao controlador de domínio, são de uso pessoal e intransferível, não sendo permitido o seu empréstimo ou compartilhamento a quem quer que seja.

21.2 A solicitação de novos usuários, redefinição de senha ou qualquer outra solicitação deverá ser feita diretamente ao Setor de Tecnologia da Informação.

22.3 Quando do ingresso de novos servidores ou estagiários o Setor de Tecnologia da Informação deverá realizar a criação do usuário e da senha provisória.

21.4 Quando do desligamento de servidores ou estagiários o Setor de Tecnologia da Informação deverá realizar imediatamente o bloqueio do usuário e da senha provisória.

21.5 O Gabinete do Diretor-Presidente poderá determinar o bloqueio temporário de acesso de servidores ou estagiários, devendo o Setor de Tecnologia da Informação realizar o bloqueio imediatamente, e somente realizar o desbloqueio após nova determinação do Gabinete do Diretor-Presidente.

22. DAS DISPOSIÇÕES FINAIS

22.1 Esta política será revisada anualmente, sendo que as alterações terão a publicidade necessária para conhecimento amplo e irrestrito.

22.2 Nos casos de dúvida o usuário poderá acionar o Setor de Tecnologia da Informação.

22.3 A presente política ficará permanentemente à disposição para conhecimento de todos, sendo que não poderá ser alegado desconhecimento para eximir-se de quaisquer responsabilidades.

**Assinatura do Documento**

Documento Assinado Eletronicamente por **HUGO LOPES DE OLIVEIRA - DIRETOR-PRESIDENTE**, **CPF:** 142.75*.**7-*0 em **27/03/2025 17:57:26**, Cód. Autenticidade da Assinatura: **1798.2357.8266.K32V.8728**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

**Informações do Documento**

ID do Documento: **5E3.12F** - Tipo de Documento: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**.

Elaborado por **HUGO LOPES DE OLIVEIRA**, **CPF:** 142.75*.**7-*0 , em **27/03/2025 17:57:26**, contendo 3.872 palavras.