POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SEROPÉDICA/RJ, 22 de dezembro de 2023.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aprovado na 54ª 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

1. 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. OBJETIVOS

2.1 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;
c) Preservar as informações do Instituto e os dados pessoais dos titulares quanto à integridade, confidencialidade e disponibilidade.

3. RISCOS

3.1 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.

3.2 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.

4. DISPONIBILIZAÇÃO, RESPONSABILIDADE E CONDUTA SOBRE OS EQUIPAMENTOS E SISTEMAS

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 É 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.

4.7 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.

4.8 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.

4.9 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.

4.10 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 .

4.11 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.

5. AÇÕES DE MONITORAMENTO E SEGURANÇA

5.1 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 a intranet, acompanhando periodicamente os acessos e logins.

6. USUÁRIO

6.1 O usuário 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.

6.2 O usuário 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.

Assinatura do Documento

Documento Assinado Eletronicamente por **HUGO LOPES DE OLIVEIRA - DIRETOR-PRESIDENTE**, **CPF:** 142.75*.**7-*0 em **22/12/2023 12:25:33**, Cód. Autenticidade da Assinatura: **1248.3E25.8336.6274.0217**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **25A.A03** - Tipo de Documento: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**.

Elaborado por **HUGO LOPES DE OLIVEIRA**, **CPF:** 142.75*.**7-*0 , em **22/12/2023 12:25:33**, contendo 1.286 palavras.

Código de Autenticidade deste Documento: 12K0.4V25.3339.V367.6008

A autenticidade do documento pode ser conferida no site: **https://zeropapel.seroprevi.rj.gov.br/verdocumento**