

FHEMIG[®]
FUNDAÇÃO HOSPITALAR DO
ESTADO DE MINAS GERAIS

Políticas Institucionais

Política de Segurança da Informação



Expediente

Presidente da Fundação Hospitalar do Estado de Minas Gerais Renata Ferreira Leles Dias

Vice Presidente Patricia Albergaria

Chefe de Gabinete Carolina Santos Lages

Diretora Assistencial Lucinéia Maria de Queiroz Carvalhais

Diretoria de Contratualização, Faturamento e Parcerias Júlia Mara Sousa Oliveira

Diretor de Planejamento, Gestão e Finanças Henrique Breguez Gonçalves Gomes Pinto Coelho

Diretor de Gestão de Pessoas Marina Emediato Lara Carvalho Mohl

Procurador Chefe João Viana da Costa

Auditora Seccional Marcela Oliveira Ferreira Dias

Assessora Estratégica Bárbara Campos de Andrade

Assessora de Comunicação Social Janaína de Oliveira

Código POL DPGF 004

Controle histórico

Versão do documento:

01

Data da elaboração:

09/10/2024

Data da revisão:

14/05/2025

Elaborado por:

Carolina Gabarra

Revisado por:

Izabella Romana

Aprovado por:

Thiago Nunes

Fundação Hospitalar do Estado de Minas Gerais

Administração Central

Cidade Administrativa de Minas Gerais | Edifício Gerais – 13º andar

Rodovia Papa João Paulo II, 4.001 - Serra Verde.

Belo Horizonte - Minas Gerais - CEP 31.630-901

www.fhemig.mg.gov.br | acs.jornalismo@fhemig.mg.gov.br

twitter.com/redefhemig | facebook.com/comunicafhemig

1. INTRODUÇÃO

A Segurança da Informação é um campo que se concentra na proteção de dados e informações contra o acesso, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição não autorizados. Seu objetivo principal é garantir confidencialidade, autenticidade, integridade e disponibilidade das informações.

Nesse sentido, a Portaria 3.201, de 12 de agosto de 2024 instituiu a Política de Segurança da Informação da Fhemig, que tem visa proteger os ativos da Fhemig, o que inclui informações de pesquisas, dados sensíveis de funcionários e pacientes, informações importantes para a execução das atividades assistenciais ou administrativas ou confidenciais.

2. OBJETIVO

A Política de Segurança da Informação da Fhemig tem vários objetivos. Primeiro, ela busca estabelecer diretrizes e normas internas para que os colaboradores adotem comportamentos seguros, alinhados com as metas da Fundação e em conformidade com as leis vigentes.

Além disso, a política orienta sobre a adoção de controles e processos necessários para garantir a segurança da informação. Isso inclui proteger informações e dados, assegurando que eles sejam confidenciais, íntegros, disponíveis e autênticos.

Outro objetivo é garantir que os princípios de proteção de dados pessoais sejam seguidos. Esses princípios incluem a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

A política também visa a gestão sistemática e eficaz dos aspectos relacionados à segurança da informação, oferecendo suporte às operações críticas e minimizando riscos e seus impactos. Por fim, ela busca prevenir possíveis incidentes, violações e responsabilizações legais.

3. ABRANGÊNCIA

Aplica-se a todos os servidores e setores da Instituição.

4. DEFINIÇÕES

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º. A Política de Segurança da Informação da Fhemig tem como objetivos:

I. Estabelecer diretrizes e normas internas de Segurança da Informação que permitam aos colaboradores da Fhemig adotar padrões de comportamento seguro, adequados às metas e necessidades da Fundação e em conformidade com as legislações vigentes;

II. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

III. Resguardar suas informações e dados, garantindo requisitos básicos de confidencialidade, integridade, disponibilidade e autenticidade;

IV. Garantir o atendimento dos princípios de proteção de dados pessoais da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas;

V. Garantir a gestão sistemática e efetiva dos aspectos relacionados à segurança da informação, provendo suporte às operações críticas e minimizando riscos identificados e seus eventuais impactos;

VI. Prevenir possíveis causas de incidentes, violações e responsabilizações legais.

Art. 2º. Aplica-se a Política de Segurança da Informação a todos os usuários dos sistemas de informação da Fhemig, seja ele nomeado, designado, contratado ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública.

Parágrafo único - O disposto no caput também a fornecedores no desempenho de atividades no ambiente lógico da Fhemig.

Art. 3º. Para os efeitos desta Portaria e seus anexos, consideram-se as definições aplicadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 4º. Para os fins desta Resolução, considera-se:

- I. access point (ponto de acesso): dispositivo que atua como ponte entre uma rede sem fio e uma rede cabeada;
- II. acesso remoto: conexão entre dispositivos (microcomputadores, servidores, etc), por meio da rede de comunicação de dados corporativa. Quando se tratar de redes corporativas distintas o mesmo deverá ser realizado por meio de VPN;
- III. administrador: contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas, normalmente não disponíveis a todos os usuários;
- IV. ambiente lógico: todo o ativo de informações da organização, incluindo pessoas, software, hardware, procedimentos e dados interagem para coletar, manipular e disseminar dados e informações;
- V. análise de riscos: processo completo de análise dos pontos críticos que possam oferecer ameaças ao ambiente tecnológico;
- VI. antimalware: ferramenta destinada a detecção, anulação e remoção de códigos maliciosos (malware);
- VII. antispyware: programa que permite identificar e remover códigos maliciosos que se auto instalam nos computadores;
- VIII. antivírus: programa que permite identificar e eliminar vírus em computadores;
- IX. ataque distribuído por negação de serviço (DDoS, do inglês Distributed Denial-of Service attack): definição semelhante ao Ataque do tipo Negação de Serviço (DoS) sendo que a diferença básica entre um ataque de DoS e de DDoS é que neste último, os ataques são realizados por diversas máquinas simultaneamente, o que aumenta a possibilidade de êxito. As máquinas utilizadas nos ataques de DDoS são denominadas zumbis;
- X. ataque do tipo negação de serviço. (DoS do inglês Denial of Service): um ataque de negação de serviço é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Não se trata de uma invasão do sistema, mas sim de provocar a sua indisponibilidade por sobrecarga;
- XI. atividades profissionais: atividades necessárias e suficientes ao desempenho das tarefas do agente público no órgão ou entidade.
- XII. autenticação: é um processo de verificação da identidade que consta em um sistema, ou seja, o sistema verifica as credenciais de quem está tentando acessar, com as que constam na base de dados, caso positivo, o sistema é liberado pois as credenciais foram validadas;
- XIII. autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui, certificada por instrumento ou testemunho público;

- XIV. backup: significa cópia de segurança. Serve para copiar dados de um dispositivo de armazenamento para outra fonte segura que poderá ser utilizada futuramente;
- XV. bring your own device (BYOD): refere-se à política de permitir que os empregados possam trazer dispositivos de propriedade pessoal (laptops, tablets e telefones inteligentes) para seu local de trabalho e usar esses dispositivos para acessar informações e aplicações dos Órgãos e Entidades;
- XVI. certificado digital: arquivo eletrônico, assinado digitalmente por uma Autoridade Certificadora, que contém dados de uma pessoa física ou jurídica, utilizados para comprovar sua identidade. O certificado digital é armazenado em uma mídia ou em um dispositivo de hardware;
- XVII. chat: palavra que em português significa “conversação” e é um neologismo para designar aplicações de conversação em “tempo real”;
- XVIII. chefia imediata: titular da área a qual está subordinado o usuário. Na sua ausência deve ser observada a ordem hierárquica superior;
- XIX. computação em nuvem: fornecimento de recursos computacionais pela internet (nuvem), sob demanda, por meio de uma plataforma de serviços;
- XX. confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;
- XXI. contas: código de acesso atribuído a cada usuário. A cada conta é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis;
- XXII. controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;
- XXIII. correio eletrônico: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;
- XXIV. criptografia: ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, por meio de um processo de cifragem e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem;
- XXV. dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- XXVI. 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;

- XXVII. diretrizes: regras de alto nível que representam os princípios básicos que a Organização resolveu incorporar a sua gestão de acordo com a visão estratégica da alta direção. Servem como base para que as normas e os procedimentos sejam criados e detalhados;
- XXVIII. disponibilidade: garantia de que os usuários autorizados obtenham acesso tempestivo (no momento da solicitação) à informação e aos ativos correspondentes;
- XXIX. dispositivo móvel: equipamentos com capacidade de armazenamento e processamento de dados, de fácil locomoção, interligados ou não à rede corporativa do órgão ou entidade, tais como notebooks, smartphones, Tablets e Coletores de Dados;
- XXX. domínio: identificação de nomes da Internet, utilizada para prover o acesso a endereços de computador, a qualquer programa de comunicação;
- XXXI. download: transferência de um arquivo de um computador para outro por meio da Internet;
- XXXII. e-mail: vide “correio eletrônico”;
- XXXIII. engenharia social: refere-se a práticas manipulativas que visam enganar indivíduos para que divulguem informações confidenciais, realizem ações prejudiciais ou forneçam acesso não autorizado a sistemas. Essa abordagem explora a natureza humana, aproveitando a confiança, a curiosidade ou o medo para atingir seus objetivos;
- XXXIV. estação de trabalho: computadores e notebooks do órgão ou entidade interligados ou não à rede corporativa;
- XXXV. ferramenta de auditoria: software que armazena os eventos gerados no ambiente computacional, permitindo a rastreabilidade da configuração e da utilização dos sistemas;
- XXXVI. firewall: é um sistema de segurança de rede que monitora e controla o tráfego de entrada e de saída da rede com base em regras de segurança pré-determinadas. Um firewall geralmente estabelece uma barreira de segurança entre uma rede interna confiável e outra rede externa, como a Internet, que se assume não segura ou confiável;
- XXXVII. 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;
- XXXVIII. gestor de segurança da informação: responsável pelas ações de segurança da informação no âmbito da Fhemig;
- XXXIX. hardware: todo e qualquer dispositivo físico em um computador;
- XL. IDS (Intrusion Detection System): sistema de detecção de intrusão que permite identificar atividades suspeitas na rede;

- XLII. incidente de segurança da informação: um ou mais eventos de segurança da informação, indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
- XLIII. integridade: salvaguarda da exatidão e completeza da informação;
- XLIV. intranet: rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os usuários possam acessar as informações dos seus respectivos Órgãos Públicos;
- XLV. IOT (Internet of Things): também conhecida como Internet das coisas, permite a detecção e controle remoto de objetos por meio de infraestrutura de rede existente, possibilitando a integração do mundo físico com sistemas baseados em computadores. Engloba tecnologias como as redes inteligentes, casas inteligentes, transporte inteligente e cidades inteligentes;
- XLVI. IPS (Intrusion Prevention System): sistema de prevenção de ataques que permite que atividades suspeitas na rede sejam bloqueadas de forma preventiva;
- XLVII. licença de software: direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes;
- XLVIII. log: arquivos que contenham informações sobre eventos de qualquer natureza em um sistema computacional com o objetivo de permitir o rastreamento de atividades;
- XLIX. login: identificação do usuário para acesso aos sistemas e serviços;
- L. logon: processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema;
- L. logout: processo de saída de um usuário dos sistemas e serviços;
- LII. malware: Software malicioso destinado a extração/alteração de informações de forma ilícita;
- LIII. mecanismos de segurança: conjunto de hardwares e softwares utilizados na implantação de regras de segurança para o ambiente;
- LIV. mídias: meio físico utilizado para armazenar dados;
- LIV. modem: equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações;
- LV. normas: especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes;
- LVI. órgão ou entidade pública: qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas;
- LVII. patch(es) - é um programa criado para atualizar ou corrigir um software;

LVIII. phishing: investida de cibercriminosos almejando a obtenção de informações pessoais, geralmente identidades online, por meio de e-mails falsos ou redirecionamentos a sites maliciosos;

LIX. política de segurança: conjunto de definições, diretrizes, restrições e requisitos que servem para nortear o uso de boas práticas no trato com os ambientes, recursos e ativos computacionais, em aspectos físicos, lógicos e de pessoal, com a finalidade de proporcionar maior segurança às informações;

LX. procedimentos: detalham no plano operacional configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas;

LXI. proteção: vide “controle”;

LXII. ransomware: É um tipo de malware (software malicioso) que tem a capacidade de tornar dados disponíveis no equipamento totalmente inacessíveis por meio de criptografia e, em seguida, solicita o pagamento de resgate em troca da chave de decodificação que é necessária para recuperar as informações contidas nos arquivos criptografados;

LXIII. recursos computacionais: recursos tecnológicos que suportam as informações do órgão ou entidade;

LXIV. rede corporativa: computadores e outros dispositivos interligados que compartilham informações ou recursos do órgão ou entidade;

LXV. rede corporativa alternativa: provimento de recursos limitados de rede sob gestão do órgão ou entidade;

LXVI. restore: recuperação de dados armazenados em cópias de segurança;

LXVII. risco: combinação da probabilidade de um evento e de suas consequências;

LXVIII. roteador: dispositivo de rede responsável por encaminhar pacotes de dados entre redes distintas criando um conjunto de redes de sobreposição;

LXIX. segurança da informação: A segurança da informação (SI) está diretamente relacionada com a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade;

LXX. senha: conjunto de caracteres utilizado para permitir a validação da identidade do usuário, a fim de tornar possível seu acesso a um sistema de informação ou serviço de uso restrito;

LXXI. serviço: sistemas e ferramentas de trabalho disponibilizados aos usuários de TIC, como correio eletrônico e acesso à Internet e intranet, acessível na rede do órgão ou entidade;

LXXII. servidor: computador responsável pelo compartilhamento de recursos e execução de serviços solicitados pelos demais computadores a ele conectados;

LXXIII. sistema corporativo: sistemas desenvolvidos para atender a gestão de toda e qualquer organização de forma integrada;

LXXIV. sistema de informação: conjunto de dados, aplicações e elementos que interagem entre si com para coletar, armazenar e processar dados e informações relacionadas às atividades da instituição.

LXXV. sistema de informação automatizado: conjunto de programas empregado para coletar, processar, transmitir e disseminar dados que representam informação para o usuário. Nesta Resolução será empregada a palavra sistema com o sentido de sistema de informação automatizado;

LXXVI. sistema operacional: programa ou conjunto de programas que responde pelo controle da alocação dos recursos do computador;

LXXVII. site: vide “sítio”;

LXXVIII. sítio: local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia;

LXXIX. software: programa de computador;

LXXX. software de comunicação instantânea: aplicação que permite o envio e recebimento de documentos diversos, imagens, mensagens de texto, vídeo e voz em tempo real;

LXXXI. spam: mensagens de correio eletrônico não solicitada, enviada em larga escala para uma lista de e-mails, fóruns ou grupos de discussão;

LXXXII. spyware: programa espião que monitora a atividade de um computador podendo transmitir estas informações a um receptor na Internet, sem o conhecimento e consentimento do usuário;

LXXXIII. streaming: tecnologia que permite a transmissão contínua de informação multimídia (áudio e vídeo) por meio de pacotes, utilizando redes de computadores, sobretudo a Internet;

LXXXIV. switch: dispositivo utilizado para interconexão de computadores, possibilitando o encaminhamento de pacotes entre os diversos nós da rede;

LXXXV. teletrabalho: o regime de trabalho no qual a atividade laboral é executada, no todo ou em parte, em local diverso daquele estabelecido para a realização do trabalho presencial, mediante a utilização de tecnologias de informação e de comunicação que permitam a execução remota das atribuições inerentes ao cargo, função ou atribuições desenvolvidas pela unidade de exercício do servidor;

LXXXVI. terceiro: pessoa jurídica ou física contratada pelo órgão ou entidade para realizar serviços;

LXXXVII. trilha de auditoria: histórico das transações dos sistemas contendo registro dos usuários que as efetuaram e das tentativas de acesso indevido;

LXXXVIII. unidade administrativa: cada área que compõe a estrutura organizacional do órgão ou entidade;

LXXXIX. upload: transferência de um arquivo, de qualquer natureza, do computador do usuário, para algum equipamento da Internet;

XC. URL (Universal Resource Locator): link ou endereço de uma página web;

XCI. userid: identificação do usuário no recurso computacional;

XCII. usuário: todo aquele que possui permissão de acesso à rede corporativa e exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em Órgão ou Entidade da Administração Pública Estadual direta ou indireta;

XCIII. vírus: programa desenvolvido com intenção nociva que, se inserido em um computador, pode causar queda do seu desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos;

XCIV. VPN (Virtual Private Network): forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tal como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação;

XCV. webmail: interface web do correio eletrônico;

XCVI. wireless: sistema de comunicação que não requer fios, funcionando por meio de equipamentos que usam radiofrequência ou comunicação via ondas de rádio para transportar sinais;

XCVII. worms: programa ou algoritmo que replica a si próprio por meio da rede e, normalmente, executa ações maliciosas, tais quais utilizar os recursos computacionais, podendo fazer com que a máquina fique indisponível.

CAPÍTULO III

DAS COMPETÊNCIAS

Art. 5º. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete às unidades administrativas e assistenciais:

- I. Auxiliar tecnicamente o Comitê Gestor de Segurança e Privacidade da Informação (CGSPI) em suas deliberações;
- II. Reportar a ocorrência de incidentes de segurança ao Comitê Gestor de Segurança e Privacidade da Informação;
- III. Tratar eventuais violações das diretrizes de segurança da Fhemig, e, quando pertinente, reportar as mesmas ao departamento de tecnologia da informação;
- IV. Solicitar, à equipe de tecnologia da informação, a concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;
- V. Solicitar a concessão ou revogação de acesso à informação ou aos sistemas de informação de acordo com os procedimentos adotados pela Fhemig;
- VI. Gerenciar as informações geradas ou sob a responsabilidade da sua área de atuação durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela Fhemig;
- VII. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de atuação conforme normas, critérios e procedimentos adotados pela Fhemig;
- VIII. Revisar periodicamente as informações geradas ou sob a responsabilidade da sua área de atuação, ajustando a classificação e rotulagem das mesmas conforme necessário;
- IX. Autorizar e revisar os acessos à informação e aos sistemas de informação sob sua responsabilidade;
- X. Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;
- XI. Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;
- XII. Revisar, anualmente, autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade;
- XIII. Classificar a informação com a finalidade de dar o tratamento adequado, de acordo com a Lei Geral de Proteção de Dados;
- XIV. Revisar, anualmente, a classificação das informações sob sua guarda; e
- XV. Controlar as informações geradas em sua área de negócio e atuação.

Art. 6º. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete à Gerência de Tecnologia da Informação e Comunicação (GTIC), ou outra que vier a substituí-la, no âmbito da Política Geral de Segurança da Informação:

- I. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- II. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- III. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;
- IV. Manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade etc.);
- V. Elaborar e cumprir cronograma de manutenção preventiva dos equipamentos;
- VI. Estabelecer e manter atualizados os procedimentos complementares a esta norma;
- VII. Receber solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de servidores, terceiros/prestadores de serviços;
- VIII. Conceder, quando autorizado, o acesso aos usuários de servidores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- IX. Revogar, mensalmente ou quando solicitado, o acesso dos usuários de servidores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- X. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de servidores, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação;
- XI. Controlar e monitorar qualquer tipo de acesso à internet fornecido pela Fhemig;
- XII. Comunicar ao CGSPI eventuais tentativas, bem-sucedidas ou não, de desvio de conduta dos termos dessa norma;
- XIII. Garantir que novas modalidades de códigos maliciosos sejam adequadamente investigados, tratados e protegidos pela ferramenta corporativa adotada pela Fhemig;
- XIV. Realizar o monitoramento dos ativos/serviços de informação ou recursos computacionais da Fhemig;
- XV. Garantir a continuidade das atividades da Fhemig com segurança, por meio da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- XVI. Manter os softwares e drivers sempre atualizados.

Art. 7º. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete à Coordenação de Gestão de Documentos (CGD), da Gerência de

Suprimentos, Logística e Patrimônio (GSLP) ou outra que vier a substituí-la, no âmbito da Política Geral de Segurança da Informação:

- I. Garantir a segurança da informação dos serviços de protocolo de documentos físicos e eletrônicos;
- II. Aplicar as melhores práticas de segurança da informação nas atividades relativas à guarda, ao tratamento e à gestão de documentos;
- III. Dar diretrizes de segurança na utilização do Sistema Eletrônico de Informações – SEI e do Sistema Integrado de Administração de Materiais e Serviços do Estado de Minas Gerais – SIAD-MG.

Art. 8º. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete à área de recursos humanos:

- I. Informar, mensalmente ou sempre que houver movimentação de pessoal, aos gestores de acesso a sistemas e à equipe de Segurança da Informação, a movimentação de pessoal no órgão ou entidade.

Art. 9º. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete à Assessoria de Comunicação:

- I. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público;
- II. Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da Fhemig.

Art. 10. Compete ao Comitê Gestor de Segurança e Privacidade da Informação (CGSPI):

- I. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSPI;
- II. Propor normas e procedimentos de segurança da informação no âmbito da Fhemig;
- III. Acompanhar e propor ações de conscientização e o treinamento dos servidores da Fhemig nos temas afetos a sua competência;
- IV. Reportar a ocorrência de incidentes de segurança ao Encarregado pelo Tratamento de Dados Pessoais.

Art. 11. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete ao responsável pela área de Segurança da Informação:

- I. Atuar como responsável por ocorrências de eventos de segurança e garantir a existência de recursos, identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;
- II. Comunicar prontamente à Equipe de resposta a incidentes de segurança da informação da Fhemig sobre eventos e incidentes de segurança.

Art. 12. Além das atribuições delimitadas pela Resolução SEPLAG nº 84/2022 ou outra que a substituir, compete ao Núcleo de Informação da Assessoria Estratégica:

- I. Gerir a arquitetura de informação organizacional de forma compatível com os objetivos institucionais da Fhemig e com padrões adequados de segurança dispostos neste documento, incluindo a definição de diretrizes para acesso aos dados;
- II. Sugerir boas práticas e estabelecer processos de utilização de dados da Fhemig, tanto para disseminação do conhecimento quanto para apoio de evidências para tomadas de decisões, visando controlar os riscos e evitar qualquer tipo de ameaça à integridade, à confidencialidade, à disponibilidade e à autenticidade desses dados;
- III. Promover a criação de estruturas analíticas, por meio do uso estratégico da tecnologia da informação e integração articulada de ferramentas de gestão informacional, como um repositório central de informações (Data Warehouse), capaz de simplificar o gerenciamento de todos os tipos de dados e oferecer maneiras diferentes de uso tendo como referência os padrões adequados de segurança dispostos neste documento;
- IV. Apoiar, avaliar e monitorar avanços tecnológicos para gestão informacional, bem como para coleta, armazenamento, análise e disseminação dessas informações tendo como referência os padrões adequados de segurança dispostos na Política de Segurança da Informação da Fhemig.

CAPÍTULO IV

DOS RECURSOS COMPUTACIONAIS

Art. 13. A Fhemig fornece os recursos computacionais necessários para que seus servidores e colaboradores executem, exclusivamente, suas atividades laborais.

Parágrafo único: O uso dos equipamentos disponibilizados pela Fhemig é de responsabilidade individual do usuário, não sendo permitido o acesso a terceiros não autorizados.

Art. 14. Os equipamentos são disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais e são de propriedade da Fhemig, sendo expressamente proibida a utilização para fins particulares.

Art. 15. No uso dos computadores, equipamentos e recursos de informática, as seguintes regras devem ser atendidas:

- I. Devem ser utilizados para uso restrito no desenvolvimento de atividades profissionais;
- II. Os usuários devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- III. É vedada a abertura e o manuseio de computadores, bem como de qualquer outro equipamento de informática, para qualquer tipo de reparo que não seja realizado por um Técnico de Informática da Fhemig ou terceiros apontados por este para execução do serviço;
- IV. Todos os modems, internos ou externos, devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas ou vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;
- V. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
- VI. Todos os recursos tecnológicos adquiridos pela Fhemig devem ter imediatamente suas senhas padrões (default) alteradas;
- VII. Os equipamentos deverão ser mantidos preservados de modo seguro, bem como os registros de eventos, constando a identificação dos usuários, datas e horários de acesso;
- VIII. Somente equipamentos autorizados pela área de Tecnologia da Informação e Comunicação (TIC) poderão se conectar à rede corporativa do órgão ou entidade.

Seção I

Da Manutenção de Hardware e Software

Art. 16. A manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de qualquer equipamento de propriedade da Fhemig é uma atribuição específica do departamento de tecnologia da informação.

Parágrafo único: A área de TIC, a seu critério exclusivo, poderá delegar a manutenção de equipamentos a outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos.

Art. 17. Toda e qualquer manutenção de Hardware e Software nos equipamentos deverá ser feita pelo usuário por meio da abertura de chamado no sistema de registro de chamados utilizado pela instituição.

Art. 18. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pela área de TI responsável.

Art. 19. A instalação, a atualização, a correção e a desinstalação de softwares devem ser realizadas pela área de TIC do órgão ou Entidade destinada a estes fins, a qual detém a guarda das credenciais de administrador dos equipamentos, e somente mediante prévia autorização da chefia imediata do usuário.

Parágrafo único: Consideram-se credencial de administrador, para os fins desta Portaria, contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas, normalmente não disponíveis a todos os usuários.

Art. 20. Os softwares sem utilização nas estações de trabalho deverão ser desinstalados.

Art. 21. Somente softwares homologados pela área responsável pela política de TIC devem ser instalados nas estações de trabalho.

Art. 22. Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Fhemig, não podendo ser interpretados como de uso pessoal.

Art. 23. Todos os softwares instalados nas máquinas devem estar de acordo com a atividade executada por seu usuário, sendo definidos pela Gerência de Tecnologia da Informação e Comunicação (GTIC).

Seção II

Dos Dispositivos Particulares

Art. 24. Entende-se por equipamento particular todo o dispositivo que não foi fornecido pelo órgão ou entidade para o desenvolvimento das atividades profissionais.

Art. 25. É permitida a utilização de dispositivo móvel particular e conexão à rede corporativa alternativa do órgão ou entidade, desde que haja uma solicitação da chefia imediata e a autorização da área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC da Fhemig.

Art. 26. O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política Geral de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito às sanções e punições previstas neste instrumento.

Art. 27. O órgão ou entidade deve definir os recursos ou dados corporativos disponíveis nos dispositivos móveis particulares.

Art. 28. A Fhemig não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais.

Art. 29. É de inteira responsabilidade do usuário a configuração do dispositivo particular conforme as regras de segurança definidas pelo órgão ou entidade. Para efeitos de gestão, os dispositivos particulares deverão ser recadastrados periodicamente. O período de recadastramento não deve ultrapassar o prazo máximo de 1 (um) ano considerando o cadastro anterior.

Art. 30. Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações da Fhemig, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir:

- I. O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;
- II. Dispositivos de computação pessoal possuem ferramenta para prevenção de códigos maliciosos e garantem que as assinaturas de códigos maliciosos são atualizadas em tempo real e executam varreduras diariamente;
- III. Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.

IV. A segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.

V. Os arquivos pessoais e/ou não pertinentes ao negócio da Fhemig (fotos, músicas, vídeos, entre outros) não sejam copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário ou chefia imediata.

Art. 31. Não é permitida a conexão de equipamentos particulares nos segmentos cabeados da infraestrutura de rede administrativa da Fhemig, sem autorização prévia formal e inspeção do equipamento tanto do departamento de tecnologia da informação, quanto da área de segurança da informação.

Art. 32. O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo particular com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.

Art. 33. O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos da Fhemig não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com a Fhemig.

Seção III

Dos Dispositivos Móveis De Propriedade Ou Alugados Pelo Órgão Ou Entidade

Art. 34. A Fhemig poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas as diretrizes:

I. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

II. Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos;

III. Os equipamentos da Fhemig devem ser utilizados com cuidado e zelo visando garantir sua preservação e seu funcionamento adequado;

IV. O usuário é responsável pelos danos decorrentes do mau uso dos dispositivos móveis sob sua responsabilidade.

Art. 35. Qualquer dano aos equipamentos da Fhemig será devidamente analisado pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá à Fhemig exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.

Art. 36. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de tecnologia da informação e é obrigatória para todos os equipamentos corporativos.

Art. 37. O dispositivo móvel será de uso e responsabilidade de seu usuário, nos termos do formulário específico assinado no momento da entrega.

Art. 38. O dispositivo móvel utilizado também fora do órgão ou entidade, deve ter suas informações armazenadas e protegidas contra acesso indevido, se possível, por meio de criptografia.

Parágrafo único. Os arquivos deverão possuir cópia no servidor do órgão ou entidade, sendo armazenados no diretório reservado à área a qual pertence o usuário responsável pelo equipamento.

Art. 39. Devem ser utilizados mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.

Art. 40. O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo cedido ou alugado com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso

será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.

Seção IV

Das Instalações Físicas e Dos Centros De Processamento de Dados

Art. 41. Terceiros nunca devem ser deixados sozinhos em áreas sensíveis, excetuando-se quando formalmente autorizado.

Parágrafo único: Área sensível é todo e qualquer espaço que contém informações que, se divulgadas ou acessadas indevidamente, podem causar danos significativos. Isso pode incluir informações pessoais, dados financeiros, detalhes de segurança, propriedade intelectual, entre outros.

Art. 42. As instalações de processamento das informações da Fhemig serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

Art. 43. Os servidores devem, sempre que possível, ser ligados a gerador de energia elétrica como “Nobreak”, para evitar que, em caso de pane elétrica, sejam danificados.

Art. 44. O local em que esteja lotado o servidor deve possuir, sempre que possível, um sistema de ar condicionado eficiente que mantenha a temperatura ideal do ambiente para o correto funcionamento dos equipamentos de TI.

Art. 45. As calhas por onde passam os fios elétricos e lógicos devem ser separados para evitar interferências.

Art. 46. O local em que esteja lotado o servidor deve possuir, sempre que possível, extintores próprios para o uso em equipamentos de TI, bem localizados, de fácil acesso e obrigatoriamente dentro da validade.

Seção V

Do Monitoramento de Sistemas de Informação

Art. 47. Toda informação que é acessada, transmitida, recebida ou produzida por meio do acesso à internet fornecido pela Fhemig está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

Art. 48. O uso dos recursos tecnológicos disponibilizados pela Fhemig é passível de monitoramento e auditoria, dispondo da análise regular de arquivos logs com utilização, quando necessário.

Art. 49. Durante o monitoramento do acesso à internet, a Fhemig se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

Art. 50. A Fhemig, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, tais como sites de proxy, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

Art. 51. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Seção VI

Das Ferramentas De Proteção

Art. 52. Apenas a ferramenta disponibilizada pela Fhemig deve ser utilizada na proteção contra códigos maliciosos.

Art. 53. A ferramenta de proteção contra códigos maliciosos da Fhemig adota as seguintes regras de uso:

I. Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;

- II. As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;
- III. As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;
- IV. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;
- V. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;
- VI. Caso uma estação de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, esta deverá ser imediatamente isolada da rede corporativa da Fhemig e de qualquer comunicação com a internet;
- VII. Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento deste da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor.

Art. 54. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no sistema de abertura de chamados.

Art. 55. Os usuários da Fhemig devem seguir as seguintes regras para proteção contra códigos maliciosos:

- I. Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
- II. Reportar imediatamente a área de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;
- III. Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
- IV. Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecidos pela Fhemig antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;

V. Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.

Art. 56. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da Fhemig devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Parágrafo único. Constitui obrigação do usuário da informação da Fhemig adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da Fundação.

CAPÍTULO V

DO TRATAMENTO DA INFORMAÇÃO

Art. 57. A Fhemig trata os dados sob custódia do órgão de forma proporcional e não excessiva, na quantidade necessária ao cumprimento de suas obrigações legais, execução de políticas públicas e regular exercício das competências previstas no Decreto nº 48.651, de 11 de julho de 2023, e outras legislações pertinentes.

Parágrafo único: O tratamento da informação deve seguir a legislação vigente, além da Política de Privacidade da Fhemig, publicada no site da instituição.

Art. 58. As informações devem ser classificadas de forma a serem protegidas adequadamente, conforme legislação prevista para cada tipo de informação no âmbito da Fhemig, levando em consideração a Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI) e a Lei Geral de Proteção de Dados;

Art. 59. Toda informação manuseada pela entidade da Administração Pública deve ter seu acesso controlado de acordo com a sua classificação, visando garantir, assim, o direito individual e coletivo das pessoas físicas ou jurídicas, a inviolabilidade de sua intimidade e o sigilo de suas informações, nos termos previstos em Lei.

Art. 60. Documentos de uso interno ou confidenciais em suporte eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas.

§ 1º Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas.

§ 2º Em períodos de ausência da estação de trabalho, documentos em suporte físico devem ser retirados das mesas e de outras áreas de superfície.

Art. 61. Cada unidade hospitalar ou diretoria deve indicar um ponto focal para tratamento de segurança da informação.

Seção I

Do Armazenamento De Informações

Art. 62. A Fhemig ainda não disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem. No entanto, disponibiliza espaço em servidores para armazenamento de arquivos localizados na PRODEMGE, para o acesso é necessário contatar a Gerência de Tecnologia da Informação.

Parágrafo único: Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela Fhemig e homologada pela equipe de segurança da informação da Fhemig.

Art. 63. Os servidores de arquivos disponibilizados na rede corporativa serão utilizados exclusivamente para armazenamento de arquivos que contenham informações relacionadas a atividades profissionais pertinentes aos processos e negócios do órgão ou entidade.

Art. 64. A seu critério exclusivo, a Fhemig poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto. Caso o usuário necessite de mais espaço, deverá realizar uma solicitação ao departamento de tecnologia da informação.

Art. 65. A utilização de dispositivos de armazenamento removível deve ser autorizada pelo gestor da informação por instrumento formal.

Art. 66. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente o departamento de segurança patrimonial para que possam ser tomadas as medidas cabíveis.

Art. 67. O descarte da informação deve ser realizado de forma a impedir a recuperação desta, independente do seu formato de armazenamento original.

Art. 68. O descarte da informação deverá ser realizado conforme os métodos estabelecidos no Anexo II desta norma.

Seção II

Do Backup

Art. 69. Os backups devem ser implementados diariamente, semanalmente, mensalmente e anualmente conforme Plano de Continuidade do negócio.

Art. 70. Todos os backups devem ser automatizados por sistema de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas janelas de backup, períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Art. 71. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta fogo segundo as normas da Associação Brasileira de Normas Técnicas - ABNT) e distantes o máximo possível do Datacenter.

Art. 72. Testes de restauração (restore) de backup devem ser executados por seus responsáveis aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Art. 73. Deve ser estabelecido um processo de gestão de risco com vistas a minimizar possíveis impactos associados aos ativos.

Art. 74. O backup e a guarda das informações armazenadas nas estações de trabalho são de responsabilidade do usuário.

Parágrafo único: Para os fins desta Portaria, estação de trabalho é todo computador ou notebook da entidade interligados ou não à rede corporativa.

Art. 75. Na existência de um servidor de arquivos administrado pela área de TIC da Fhemig, este deve ser utilizado como ponto central para armazenamento das informações pertinentes à atividade exercida.

Art. 76. Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Seção III

Dos Bancos de Dados

Art. 77. Utilizar criptografia para os dados do banco de dados e para os dados de credenciais.

Art. 78. Monitorar as atividades dos usuários.

Art. 79. Aplicar os mesmos controles de segurança do próprio banco de dados aos backups.

Parágrafo único: Realizar testes de validação e desempenho das cópias de segurança.

Seção IV

Do Tratamento de Informações Assistenciais

Art. 80. A digitalização de documentos deve seguir o disposto pelas Lei nº 13.874, de 20 de setembro de 2019, Lei nº 13.787, de 27 de dezembro de 2018, e pelo Decreto nº 10.278, de 18 de março de 2020, e suas alterações.

Art. 81. O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a rastreabilidade, a interoperabilidade, a autenticidade e a confidencialidade do documento digital.

Art. 82. Parágrafo único: A digitalização de prontuários deve assegurar cumprimento integral à Lei Geral de Proteção de Dados (LGPD).

Art. 83. Os métodos de digitalização devem reproduzir todas as informações contidas nos documentos originais.

Art. 84. No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito.

Art. 85. Os documentos originais poderão ser destruídos após a sua digitalização, ressalvados aqueles com conteúdo de valor histórico.

Art. 86. Os meios de armazenamento de documentos digitais deverão protegê-los do acesso, do uso, da alteração, da reprodução e da destruição não autorizados.

Art. 87. Os documentos oriundos da digitalização de prontuários de pacientes serão controlados por meio de sistema especializado de gerenciamento eletrônico de documentos, cujas características e requisitos serão especificados na portaria.

Art. 88. O documento digitalizado em conformidade com as normas estabelecidas na Lei terá o mesmo valor probatório do documento original para todos os fins de direito.

Art. 89. Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados.

Art. 90. O processo de eliminação deverá resguardar a intimidade do paciente e o sigilo e a confidencialidade das informações.

Art. 91. Os dados dos pacientes devem trafegar na rede mundial de computadores (internet) com infraestrutura, gerenciamento de riscos e os requisitos obrigatórios para assegurar registro digital apropriado e seguro, obedecendo às normas do CFM pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade e à garantia do sigilo profissional das informações.

Art. 92. A guarda das informações relacionadas aos documentos emitidos deve atender a legislação vigente e estar sob responsabilidade do médico incumbido pelo atendimento. Nos estabelecimentos de saúde essa responsabilidade será compartilhada com o diretor técnico das instituições e/ou da plataforma eletrônica.

CAPÍTULO VI DO ACESSO

Art. 93. Além das disposições da Resolução SEPLAG nº 84/2022 ou outra que a substituir, a concessão de acesso à rede corporativa da Fhemig deve observar:

I. A concessão de acesso à rede corporativa do órgão ou entidade será realizada mediante solicitação formal dos responsáveis pela área do usuário por meio do Formulário de Acesso aos Sistemas.

II. Os usuários e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Tecnologia da Informação.

Parágrafo único: O Formulário de Acesso aos Sistemas deve ser encaminhado via SEI, pelo formulário padronizado “RH - Formulário Acesso aos Sistemas - Fhemig”, ou outro que o substituir, para a unidade FHEMIG/DPGF/GTIC/CSMTIC, ou outra que a substituir.

Art. 94. O Formulário de Acesso aos Sistemas deve ser assinado pela chefia imediata.

Art. 95. Os acessos dos usuários desligados deverão ser bloqueados ou revogados no momento em que o desligamento for informado pela área de Recursos Humanos ou chefia imediata.

Art. 96. Deverão ter seus acessos bloqueados os usuários em licença ou afastamento superior a 90 (noventa) dias.

Art. 97. Toda conta é de responsabilidade e uso exclusivo de seu titular. As contas inativas por mais de 180 (cento e oitenta) dias serão desativadas, conforme política de bloqueio e exclusão de contas. O usuário que quiser preservar seus dados deverá comunicar a GTIC seu afastamento com antecedência mínima de 30 (trinta) dias.

Parágrafo único: A política de bloqueio e exclusão de contas será definida pelo CGSPI.

Seção I

Do Certificado Digital

Art. 98. A Fhemig poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que executam atividades profissionais específicas.

Art. 99. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

Art. 100. O usuário deverá informar à equipe de segurança da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital.

Seção II

Do Acesso Remoto

Art. 101. Disponibilizar-se-á ao usuário o acesso remoto somente por meio de VPN ou outro meio aprovado pelo órgão para a execução de atividades relacionadas ao órgão ou entidade. Parágrafo Único - O órgão ou entidade reserva para si o direito de monitorar a utilização do acesso remoto disponibilizado.

Art. 102. O acesso remoto à rede corporativa em locais públicos deve ser evitado.

Art. 103. É vedada a utilização de ferramentas de nuvem e de comunicação instantânea que não sejam fornecidas pela Fhemig.

Seção III

Do Acesso à Internet

Art. 104. A Fhemig fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais.

Art. 105. As diretrizes para o uso da internet visam o desenvolvimento de um comportamento eminentemente ético e profissional.

§1º O usuário deverá utilizar a Internet em conformidade com a lei, a ordem pública e o Código de Conduta Ética do Agente Público e da Alta Administração Estadual.

§2º É facultado ao usuário o emprego da Internet para a melhoria de sua qualificação profissional ou para acesso a serviços, tais como Internet Banking e similares.

Art. 106. Para a utilização da internet, recomenda-se:

- I. Manter o navegador web atualizado;
- II. Atentar para a autorização de cookies;
- III. Certificar-se da procedência do site e da utilização de conexões seguras; e
- IV. Analisar os “Termos e Condições” com atenção.

Art. 107. É vedada a realização de upload de qualquer software ou dados de propriedade do órgão ou entidades do governo do Estado sem a autorização expressa da área de Segurança da Informação.

Parágrafo único: A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada se atendidos todos os requisitos:

- I. Se for verificada positivamente;
- II. Se estiver de acordo com a classificação de tal informação;
- III. Com a real necessidade do destinatário;
- IV. Com a devida identificação do solicitante.

Art. 108. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede.

Parágrafo único: O desbloqueio de site que está de acordo com as diretrizes de utilização da internet, poderá ser feito mediante solicitação do usuário à Coordenação de Infraestrutura de TIC Gerência de Tecnologia da Informação e Comunicação.

Seção IV

Dos Acessos Privilegiados

Art. 109. O acesso a ativos/serviços de informação é fornecido a critério da Fhemig, que define permissões baseadas nas necessidades laborais dos usuários.

Art. 110. Deve-se atribuir o menor privilégio possível a uma conta, que deverá permitir apenas a realização das tarefas pertinentes ao seu usuário.

Parágrafo único: A autorização e o nível permitido de acesso ativos/serviços de informação da Fhemig é feita com base em perfis que definem o nível de privilégio dos usuários.

Art. 111. Usuários que têm acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito.

Parágrafo único: A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia.

Art. 112. A concessão e o uso de privilégios serão restritos, autorizados e controlados por meio de um processo de gerenciamento formal pelo Administrador do Sistema.

Parágrafo único: Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas à equipe de tecnologia da informação.

Seção V

Das Senhas

Art. 113. Cada usuário deverá possuir uma conta individual e uma senha que seja pessoal e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis e assegurando que não utilize de maneira indevida a sua senha.

Parágrafo único: A senha individual e intransferível é indispensável para a apuração de responsabilidades.

Art. 114. Além dos requisitos da Resolução SEPLAG nº 84/2022 ou outra que a substituir, as senhas dos sistemas de informação gerenciados pela Fhemig devem observar:

I. As senhas associadas a contas que possuem privilégio administrativo serão compostas de quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

II. Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo por, no mínimo, 30 (trinta) minutos;

III. Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da equipe de tecnologia da informação.

Art. 115. As senhas para acesso à rede corporativa serão armazenadas e transmitidas criptografadas.

Art. 116. É vedado o compartilhamento de senhas.

Art. 117. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, incumbindo uma análise da infração pelo CGSPI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

Seção VI

Do Aviso Legal

Art. 118. A Fhemig faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso a ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas pela Fhemig, bem como do monitoramento realizado nos termos desta norma.

Art. 119. O aviso legal deverá ser exibido antes de permitir o acesso a ativos/serviços de informação ou recursos computacionais da Fhemig, apresentando o seguinte formato:

Este é um ativo/serviço de informação ou recurso computacional da Fhemig, o qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste sistema, o infrator estará sujeito a sanções cabíveis nas esferas administrativa, cível e penal, sem prejuízo das demais legislações aplicáveis. Este ativo/serviço de informação ou recurso computacional é monitorado, não havendo expectativa de privacidade na sua utilização. O acesso a este ativo/serviço de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos.

Art. 120. O acesso a qualquer ativo/serviço de informação ou recurso computacional da Fhemig ou o uso dos mesmos por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal.

Art. 121. A ausência do aviso legal em qualquer ativo/serviço de informação ou recurso computacional da Fhemig não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pela Fhemig.

CAPÍTULO VII

DAS DIRETRIZES DE SEGURANÇA

Seção I

Das Vedações

Art. 122. É vedado aos usuários:

- I. Realizar procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Tecnologia da Informação e Comunicação, ou de quem este determinar;
- II. Fazer uso de contas de e-mail pessoal para tratamento de demandas corporativas;
- III. Compartilhar senhas;
- IV. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- V. Burlar quaisquer sistemas de segurança;
- VI. Acessar informações confidenciais sem explícita autorização do proprietário;
- VII. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- VIII. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- IX. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- X. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- XI. Utilizar os recursos computacionais da Fhemig para efetuar trabalho de natureza particular;

- XII. Conectar equipamentos computacionais na Rede que não sejam de propriedade da Fhemig, tais como notebooks, tablets e smartphones, sem a autorização prévia do Comitê Gestor de Tecnologia da Informação;
- XIII. Movimentar equipamento, bem como trocar periféricos sem a prévia autorização da área de TIC;
- XIV. Usar modems e/ou roteadores para conexões externas dentro das dependências da Fhemig sem prévia autorização do Comitê Gestor de Tecnologia da Informação;
- XV. Instalar softwares sem a devida autorização do departamento de tecnologia da informação;
- XVI. Utilizar modem de banda larga no ambiente dos órgãos e entidades que disponibilizam acesso à rede corporativa;
- XVII. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional vigente.

Seção II

Do Correio Eletrônico

Art. 123. Além das disposições da Resolução SEPLAG nº 84/2022 ou outra que a substituir, é vedado ao usuário, no uso da conta de correio eletrônico:

- I. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;
- II. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- III. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Fhemig ou suas unidades vulneráveis a ações civis ou criminais;
- IV. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- V. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- VI. Abrir mensagens de correio eletrônico cujo assunto ou remetente sejam de origem desconhecida ou suspeita;
- VII. Executar arquivos e anexos de origem desconhecida ou suspeita.

- VIII. Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Fhemig estiver sujeita a algum tipo de investigação;
- IX. Usar contas particulares dos usuários, por meio dos serviços Post Office Protocol - POP, Internet Message Access Protocol - IMAP e Simple Mail Transfer Protocol - SMTP de provedores não pertinentes ao domínio fhemig.mg.gov.br;
- X. Enviar, armazenar e manusear material que contrarie o disposto na legislação vigente, a moral, os bons costumes e a ordem pública;
- XI. Enviar, armazenar e manusear material que caracterize divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- XII. Enviar mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade da Fhemig;
- XIII. Produzir, transmitir, divulgar, armazenar, manusear mensagem ou material que:
- a. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Fhemig;
 - b. Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador, etc;
 - c. Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
 - d. Caracterize promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas e assuntos de caráter obsceno;
 - e. Vise obter acesso não autorizado a outro computador, servidor ou rede;
 - f. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
 - g. Vise burlar qualquer sistema de segurança;
 - h. Vise vigiar secretamente ou assediar outro usuário;
 - i. Vise acessar informações confidenciais sem explícita autorização do proprietário;
 - j. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
 - k. Inclua imagens criptografadas ou de qualquer forma mascaradas;
 - l. Tenha conteúdo considerado impróprio, obsceno ou ilegal;
 - m. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;

- n. Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- o. Tenha fins políticos locais ou do país (propaganda política);
- p. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Art. 124. Para a utilização da ferramenta de correio eletrônico, recomenda-se:

- I. Utilizar linguagem clara, para evitar ruídos de interpretação;
- II. Verificar a seleção de todos os destinatários necessários;
- III. Rer a mensagem antes do envio;
- IV. Evitar o anexo de arquivos grandes ao e-mail corporativo; e
- V. Conferir o recebimento de e-mails periodicamente.

Parágrafo único: O padrão para criação de contas é a utilização do primeiro nome do titular e seu último nome. (Exemplo: Nome fictício: José Luiz da Silva - Login: jose.silva@fhemig.mg.gov.br). Caso haja nomes repetidos, deve-se utilizar outro sobrenome. Caso utilize o ExpressoMg ou plataforma/software que vier a substituí-lo para acesso a criação de contas de e-mail, o Login será o CPF do usuário solicitante.

Art. 125. O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico.

Art. 126. O uso do correio eletrônico da Fhemig é para fins corporativos e relacionados às atividades do usuário no âmbito da instituição.

Seção III

Dos Comunicadores Instantâneos

Art. 127. A Fhemig fornece o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais.

Art. 128. Não é permitido o uso de qualquer serviço de comunicadores instantâneos, mensageiros instantâneos ou programas de computador que permitam a comunicação imediata e direta entre usuários e grupos de usuários por meio da Internet, tais como Facebook, Whatsapp, Instagram e afins, exceto o mensageiro instantâneo corporativo ou quando solicitado e autorizado pela área de Segurança da Informação;

Art. 129. Quando o usuário fizer uso do serviço de comunicadores instantâneos da Fhemig, não é permitido:

- I. Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de interesse da Fhemig;
- II. Trafegar imagens e arquivos pesados, que possam impactar no desempenho do servidor.

Seção IV

Da Participação em Videoconferências

Art. 130. É permitida a participação dos agentes públicos em videoconferência utilizando a Internet, para tratar de assuntos corporativos.

Art. 131. Para a participação em videoconferências, recomenda-se:

- I. Ser pontual ao horário da reunião;
- II. Não divulgar o link de participação em locais públicos, para evitar invasões;
- III. Definir um moderador para autorizar entrada de participantes e para introduzir a pauta;
- IV. Em caso de gravação, solicitar aprovação dos participantes;
- V. Manter o microfone desligado enquanto não estiver falando; e
- VI. Testar os periféricos antes do início da videoconferência.

Art. 132. O uso da ferramenta corporativa ExpressoMg, ou outra que vier a substituí-la, é obrigatório para realização de reuniões virtuais.

Parágrafo Único - Excepcionalmente, outras ferramentas poderão ser utilizadas para a realização de reuniões virtuais. Elas se encontram liberadas para uso na rede corporativa por meio dos navegadores web.

Seção V

Das Mídias Sociais

Art. 133. A publicação de conteúdo referente à Fhemig em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização.

Art. 134. Quando no uso de suas mídias e redes sociais particulares, servidores, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

I. Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da Fhemig sem autorização prévia e expressa da Assessoria de Comunicação Social, ou outra que vier a substituí-la;

II. Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da Fhemig, excetuando-se os canais oficiais da empresa;

III. Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à Fhemig, seus empregados, terceiros contratados e prestadores de serviço;

IV. Não é permitida a fotografia, a filmagem e a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da Fhemig, aos pacientes e a seus dados, sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

CAPÍTULO VII

DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 135. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da Fhemig serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

Parágrafo único: Toda não-conformidade será tratada como um incidente de segurança da informação, incumbindo análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

Art. 136. Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista.

Art. 137. Os incidentes de segurança devem ser reportados através dos canais administrativos adequados o mais rapidamente possível. É dever de todos comunicar imediatamente à

Gerência de Tecnologia da Informação qualquer descumprimento da Política de Segurança da Informação.

Art. 138. A área de segurança da informação deverá determinar a criticidade do incidente e comunicar às partes interessadas, em especial ao Encarregado de Dados e aos membros do time de resposta a incidentes de segurança da informação.

Art. 139. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente.

Art. 140. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para a erradicação completa do incidente e restauração dos ativos de informação afetados.

Art. 141. Qualquer tentativa de acesso indevido identificado será tratada como incidente de segurança.

Art. 142. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

ART. 143. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas à Fhemig sem aprovação expressa e formal da assessoria de comunicação.

Art. 144. Todas as Notificações de Incidentes de Segurança deverão ser devidamente informadas às chefias responsáveis, se possível divulgadas para todos os servidores, e seu registro deverá ser mantido por pelo menos 05 anos.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 145. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.

Art. 146. O usuário que não cumprir as normas estabelecidas nesta Portaria estará sujeito às penalidades previstas em Lei, notadamente a Lei Geral de Proteção de Dados e o Estatuto do Servidor Público de Minas Gerais.

Art. 147. Usuários que fizerem uso indevido de recursos da Rede poderão ter seu acesso bloqueado temporariamente ou definitivamente, após notificação.

Parágrafo único. No caso de terceiros contratados ou prestadores de serviço, o CGSPI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Art. 148. Esta política será revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação, para garantir sua contínua pertinência e adequação às necessidades da FHEMIG.

Art. 149. Os casos omissos desta portaria serão deliberados pelo Comitê Gestor de Segurança e Privacidade da Informação.

5. RESPONSABILIDADES

Gerência de Tecnologia da Informação e Comunicação (GTIC)

6. O PAPEL DO PACIENTE

O paciente desempenha um papel fundamental na promoção e manutenção da Segurança da Informação dentro da instituição. Algumas ações possíveis:

- Respeitar as normas e orientações do Marco Civil da Internet;
- Manter a confidencialidade de seus dados de acesso a sistemas (quando aplicável), como senhas ou códigos de autenticação, não os compartilhando com terceiros;
- Informar à equipe responsável qualquer situação suspeita envolvendo seus dados pessoais, como acesso não autorizado ou tentativa de obtenção de informações por terceiros;

- Exercer seus direitos garantidos pela legislação vigente, como a Lei Geral de Proteção de Dados (LGPD), de forma consciente e colaborativa.

7. METAS E INDICADORES

NA

8. SIGLAS

CD - Compact Disc (Disco Compacto)

CFM - Conselho Federal de Medicina

CGD - Coordenação de Gestão de Documentos

CGSPI - Comitê Gestor de Segurança e Privacidade da Informação

DAT - Digital Audio Tape (Fita de Áudio Digital)

DDoS - Distributed Denial of Service attack (Ataque Distribuído do tipo Negação de Serviço)

DLT - Digital Linear Tape (Fita Linear Digital)

DoS - Denial of Service attack (Ataque do tipo Negação de Serviço)

DVD - Digital Versatile Disc (Disco Versátil Digital)

GSLP - Gerência de Suprimentos, Logística e Patrimônio

GTIC - Gerência de Tecnologia da Informação e Comunicação

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira

IDS - Intrusion Detection System (Sistema de Detecção de Intrusão)

IMAP - Internet Message Access Protocol (Protocolo de Acesso a Mensagens da Internet)

IOT - Internet of Things (Internet das Coisas)

IPS - Intrusion Prevention System (Sistema de Prevenção de Intrusão)

LGPD - Lei Geral de Proteção de Dados

LTO - Linear Tape-Open (Fita Linear Aberta)

POP - Post Office Protocol (Protocolo dos Correios)

SEI - Sistema Eletrônico de Informações

SEPLAG - Secretaria de Estado de Planejamento e Gestão

SIAD-MG - Sistema Integrado de Administração de Materiais e Serviços do Estado de Minas Gerais

SMTP - Simple Mail Transfer Protocol (Protocolo de Transferência de Correio Simples)

TI - Tecnologia da Informação

URL - Universal Resource Locator (Localizador Universal de Recursos)

VPN - Virtual Private Network (Rede Privada Virtual)

9. REFERÊNCIAS BIBLIOGRÁFICAS

FUNDAÇÃO HOSPITALAR DO ESTADO DE MINAS GERAIS. **Portaria nº 3.201, de 12 de agosto de 2024.** Institui a Política de Segurança da Informação no âmbito da Fundação Hospitalar do Estado de Minas Gerais. Disponível em: [https://www.pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=211461&marc=.](https://www.pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=211461&marc=) Acesso em: 10 out. 2024.

10. ANEXOS

NA



Planejamento
Estratégico



Fundação Hospitalar do Estado de Minas Gerais

FHEMIG | Cidade Administrativa de Minas Gerais

Edifício Gerais - 13º andar

Rodovia Papa João Paulo II, 4.001 - Serra Verde.

Belo Horizonte - Minas Gerais - CEP 31.630-901

Telefone (31) 3915-9500

-  www.fhemig.mg.gov.br
-  [@redefhemig](https://www.instagram.com/redefhemig)
-  [facebook.com/comunicafhemig](https://www.facebook.com/comunicafhemig)
-  twitter.com/redefhemig