FUNDAFFEMG

NOSSO PLANO É VIDA E SAÚDE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ADMINISTRAÇÃO 2019/2021

DIRETORIA EXECUTIVA

Diretor Presidente
Munir Nacif Mitre

Diretor Administrativo e Financeiro
Luiz Antônio Ribeiro

Diretor de Assistência à Saúde
Antônio Caetano Jacinto Lemos

Assessora da Diretoria Executiva
Fátima Taher Jounis

CONSELHO CURADOR

Membros do Conselho Curador Efetivos

Carolina Amália C. Monteiro André
Edir da Silva Martins
Edvaldo Ferreira
Flávio Lima de Oliveira
Jânio Ramos
José Agnaldo Viegas Barbosa
José Aparecido de Pádua
José Gomes Soares
Jussara Elias Gualberto
Roberto Borges
Ronan Andrade de Oliveira
Sara Costa Felix Teixeira

Membros do Conselho Curador Suplentes

Astolfo Geraldo de Andrade
Lúcia Martins Perissé
Luiz Antunes Eustáquio
Maria de Lourdes Medeiros
Mônica Schusterschitz da Silva Araújo
Vera Maria Sampaio Teixeira Zambelli Loyola

CONSELHO FISCAL

Membros do Conselho Fiscal Efetivos

Iracema Ceci Amaral Renan
José Guilhermino Barbosa Filho
José Luiz de Lima

Membros do Conselho Fiscal Suplentes

Adevaldo Antônio de Catro
Hercília Maria de Almeida José
Najla de Paula Cruz

COMISSÃO DE ELABORAÇÃO

Gestora de Auditoria Médica
Márcia Mariano

Gestora de TI
Nathália Góes

Gestora de Compliance
Simone Lima dos Santos

Histórico de Versões

Data	Versão	Descrição	Autor
31/12/2020	1.0	Primeira versão da Política de Segurança da Informação	Comissão Portaria 02/2020

ÍNDICE

1. INTRODUÇÃO

A governança no compartilhamento de dados na FUNDAFFEMG segue as diretrizes estabelecidas no Art. 7º da Resolução Normativa - RN n° 443 de 25 de janeiro de 2019, Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES da Agencia Nacional de Saúde- ANS, indicações de boas práticas contidas nas Normas ABNT: ISO 27001 – Sistema de Gestão de Segurança da Informação; ISO 27002 – Controles de Segurança da Informação; ISO 38500 – Governança de TI; ISO 31000 – Gestão de Riscos; ISO 27005 – Gestão de Riscos de Segurança da Informação e precisa ser compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicação e ainda o disposto pela Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Nesse contexto, este documento tem como objetivo estabelecer as diretrizes adotadas na segurança da informação na FUNDAFFEMG para as operações envolvendo o tratamento de dados pessoais, conforme previsto no art. 50 da LGPD, assim como todo o arcabouço de dados e informações utilizados e trafegados no âmbito do negócio de saúde suplementar.

Inicialmente, a adequação da Fundação em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação envolve: considerar a privacidade dos dados pessoais do Beneficiário/funcionário/ prestador de serviço ou qualquer pessoa cujo dado pessoal seja tratado na FUNDAFFEMG, desde a fase de concepção do serviço até sua execução (Privacidade by Design); e promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Cumpre destacar que o princípio da finalidade do tratamento de dados estabelecido na LGPD exige que os propósitos do tratamento sejam legítimos, específicos, explícitos e informados ao titular do dado. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades (art. 6º, I). No caso do setor da saúde suplementar, a finalidade relaciona-se com a execução da regulação ANS, legislação dos Conselhos dos Profissionais de Saúde, assim como os ditames da Consolidação das Leis Trabalhistas _CLT, e com o cumprimento de obrigação legal ou regulatória pelo controlador. O consentimento, quando necessário, será medida excepcional e deverá se referir a finalidades determinadas e comunicadas claramente ao titular do dado.

2. DEFINIÇÕES

Para efeito desta política considera-se:

Titular[1]: (Ref.: Lei 13.709/2018) pessoa natural a quem os dados pessoais que são objeto de tratamento;

Agentes de Tratamento[2]: (Ref.: Lei 13.709/2018) Controlador, Operador, Encarregado;

Controlador: (Ref.: Lei 13.709/2018) pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. A FUNDAFFEMG configura um controlador na pessoa de seus representantes legais, assim como o prestador de serviço ou fornecedor;

Operador: (Ref.: Lei 13.709/2018) pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais ou não em nome do controlador. São operadores: os colaboradores da FUNDAFFEMG no exercício de sua função são operadores e tratam a informação digital, eletrônica, escrita e falada, assim como os funcionários de nossos pares e parceiros;

Encarregado: (Ref.: Lei 13.709/2018) pessoa designada pela Diretoria Executiva que representa concomitantemente o papel de controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Dado pessoal[4]: (Ref.: Lei 13.709/2018) informação relacionada a pessoa natural identificada ou identificável;

---

1. Proprietário da informação pessoal. (Pessoa física natural cuja informação o identifica, como o CPF por exemplo)

2. Agente de Tratamento: Se aplica tanto a instituição Fundaffemg ou prestador de serviço, Fornecedor, etc. quanto ao colaborador da Fundaffemg ou do prestador de serviço cuja função seja tratar a informação recebida ou enviada.

3. Segundo a LGPD, tratamento de dados pessoais é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4. Além das informações básicas relativas ao nome, número de inscrição no Registro Geral (RG) ou no Cadastro Nacional de Pessoas Físicas (CPF) e endereço residencial, são também considerados dados pessoais outros dados que permitam a identificação de um indivíduo, tais como a orientação sexual, a filiação político-partidária, o histórico médico e também aqueles referentes aos seus aspectos biométricos. Segundo a LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Dado pessoal sensível: (Ref.: Lei 13.709/2018) 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;

Dado anonimizado: (Ref.: Lei 13.709/2018) dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Banco de dados: (Ref.: Lei 13.709/2018) conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Armazenamento: (Ref.: Guia Boas Práticas Adm.Federal) ação ou resultado de manter ou conservar em repositório um dado;

Arquivamento: (Ref.: Guia Boas Práticas Adm.Federal) ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;

Avaliação: (Ref.: Guia Boas Práticas Adm.Federal) analisar o dado com o objetivo de produzir informação;

Classificação: (Ref.: Guia Boas Práticas Adm.Federal) maneira de ordenar os dados conforme algum critério estabelecido;

Coleta: (Ref.: Guia Boas Práticas Adm.Federal) recolhimento de dados com finalidade específica;

Comunicação: (Ref.: Guia Boas Práticas Adm.Federal) transmitir informações pertinentes a políticas de ação sobre os dados;

Controle: (Ref.: Guia Boas Práticas Adm.Federal) ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

Difusão: (Ref.: Guia Boas Práticas Adm.Federal) ato ou efeito de divulgação, propagação, multiplicação dos dados;

Distribuição: (Ref.: Guia Boas Práticas Adm.Federal) ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

Eliminação: (Ref.: Guia Boas Práticas Adm.Federal)- ato ou efeito de excluir ou destruir dado do repositório;

Extração: (Ref.: Guia Boas Práticas Adm.Federal) ato de copiar ou retirar dados do repositório em que se encontrava;

Modificação: (Ref.: Guia Boas Práticas Adm.Federal) ato ou efeito de alteração do dado;

Processamento: (Ref.: Guia Boas Práticas Adm–.Federal) ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

Recepção: (Ref.: Guia Boas Práticas Adm.Federal) ato de receber os dados ao final da transmissão;

Reprodução: (Ref.: Guia Boas Práticas Adm.Federal) cópia de dado preexistente obtido por meio de qualquer processo;

Transferência: (Ref.: Guia Boas Práticas Adm.Federal) mudança de dados de uma área de armazenamento para outra, ou para terceiro (prestador de serviço/fornecedor ou beneficiário);

Transmissão: (Ref.: Guia Boas Práticas Adm.Federal) movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

Utilização: (Ref.: Guia Boas Práticas Adm.Federal) ato ou efeito do aproveitamento dos dados;

Gestão de Segurança da Informação: (Ref.: ISO 27001) – Conjunto de medidas que visam à proteção dos ativos de segurança da informação;

Gestão de Riscos: (Ref.: ISO 27005 E ISO 31000) – Conjunto de medidas que buscam atenuar os riscos da informação, identificados por meio critérios pré-estabelecidos na política de Gestão de Riscos da FUNDAFFEMG. A Análise de Risco será feita sempre que houver pauta do tema submetido ao Comitê, emitindo relatório, quando necessário, para apresentação e julgamento da Diretoria;

Plano de Continuidade de Negócio (Ref.: ISO 27005) – Plano desenvolvido através da identificação de causas que possam afetar a disponibilidade dos serviços, propondo alternativas para seu restabelecimento, visando garantir a não interrupção dos serviços críticos nos ambientes computacionais;

Plano de Ação e Resposta a Incidentes: (Ref.: ISO 27001 / ISO 22301) – documento com orientações e procedimentos que devem ser realizados em situações de suspeita, denúncia e constatação de fraude no sistema e violação de dados;

Relatório de Impacto à Proteção de Dados Pessoais: (Ref.: Lei 13.709/2018) Documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados;

Segundo o inciso XVII do art. 5º da LGPD, o RIPD é documentação que deve ser mantida pelo Encarregado.

> *Art. 5º Para os fins desta Lei, considera-se:*
> *XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

Enquanto o art. 5º inciso XVII define o que é um RIPD, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, grifado abaixo.

> *Art. 38.* ***A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais****, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Proprietário da Informação: É o responsável pela autorização do acesso a ela. No exercício laboral na FUNDAFFEMG o responsável[5] por essa autorização é o gestor de unidade.

5. O proprietário da informação no âmbito da Fundaffemg é gestor em razão de termos a posse do Termo de Consentimento do beneficiário que é o titular do dado e nos autorizou a trata-la.

3. DIRETRIZES BÁSICAS

1. Assegurar a confidencialidade, integridade e disponibilidade das informações da Fundação, mediante utilização de mecanismos de segurança da informação e cibernética, balanceando fatores de risco, tecnologia e custo;

2. Garantir a proteção adequada das informações e dos sistemas contra acesso indevido, cópia, leitura, modificação, destruição e divulgação não autorizados;

3. Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Fundação, estando sujeitos à monitoração, rastreabilidade e auditoria;

4. Assegurar a existência de processos para continuidade de negócios e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra ataques cibernéticos;

5. Informar aos beneficiários, prestadores de serviços, funcionários, candidatos a processo seletivo, temporários, enfim a todo operador da informação digital, escrita ou verbal sobre as precauções de Segurança da Informação e Cibernética necessárias na utilização de dados e informações tratados no âmbito da saúde suplementar;

6. Garantir o cumprimento desta Política, das Normas e Padrões Corporativos de Segurança da Informação da Fundação;

7. Assegurar o comprometimento da alta administração com a melhoria contínua dos processos e recursos necessários para Segurança da Informação e Cibernética.

A Política de Segurança da Informação é uma declaração formal da Instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, prestadores de serviços e quaisquer agentes de tratamento, seja ela de propriedade do titular do dado ou não, observando sempre o instituto do art. 5º da Lei Federal 13.709/2018 e sua relação com o negócio da FUNDAFFEMG.

4. COMPOSIÇÃO DA PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA FUNDAFFEMG

4.1 Estrutura Normativa e Sua Revisão

A estrutura da PSI é composta por um conjunto de documentos que observam a hierarquia a seguir, iniciando dos pilares da política e chegando até o detalhamento operacional nessa ordem:

1. Política de Segurança da Informação - Constituída por este documento define a estrutura, as diretrizes e as obrigações referentes à segurança da informação. A revisão cabe ao encarregado designado nos termos da Lei Federal 13.709/2018, subsidiado pelo Comitê Gestor da Segurança da Informação designado por meio de Portaria da Diretoria Executiva. A aprovação final deste documento é de competência exclusiva da Diretoria Executiva. Sua revisão deverá ser anual ou extraordinária sempre que ocorrer, alterações na legislação aplicável e seleção de melhores práticas recomendadas pela Associação Brasileira de Normas Técnicas (ABNT);

2. Normas de Segurança da Informação - Descrevem as regras de segurança definidas de acordo com as diretrizes desta Política, a serem seguidas em todas as situações em que a informação é tratada. É de responsabilidade do Encarregado, subsidiado pelo Comitê Gestor da Segurança da Informação da FUNDAFFEMG, a pré-aprovação da norma bem como sua submissão à aprovação da Diretoria Executiva. Cabe ao Encarregado a revisão e atualização sistemática dessas, buscando as melhores práticas de um Sistema de Gestão de Segurança da Informação – SGSI (referencia: ISO 27001);

3. Procedimentos de Segurança da Informação - Visam instrumentalizar o disposto nas Normas e na Política. Cabe ao Gestor de Tecnologia da Informação elaborar os procedimentos de segurança de dados e cibernética, adotados. Os demais procedimentos operacionais padrão desafetos à questão tecnológica, porém relacionados ao tratamento da informação caberá ao Encarregado a construção conjunta com o Gestor de cada unidade, sempre observando as melhores práticas indicadas pelas normas ABNT: ISO 27002 – Controles de Segurança da Informação; ISO 38500 – Governança de TI; ISO 27701 – Sistema de Gestão de Informações Privadas; ISO 27701 – Sistema de Gestão de Informações Privadas e também a COBIT - Control Objectives for Information and related Technology. Os procedimentos operacionais deverão ser atualizados, aperfeiçoados, ampliados permanentemente, considerando a familiarização com o novo universo da proteção e tratamento de dados pessoaisuma vez que algumas diretrizes de proteção de dados da LGPD estão sujeitas à regulamentação Autoridade Nacional de Proteção de Dados-ANP.

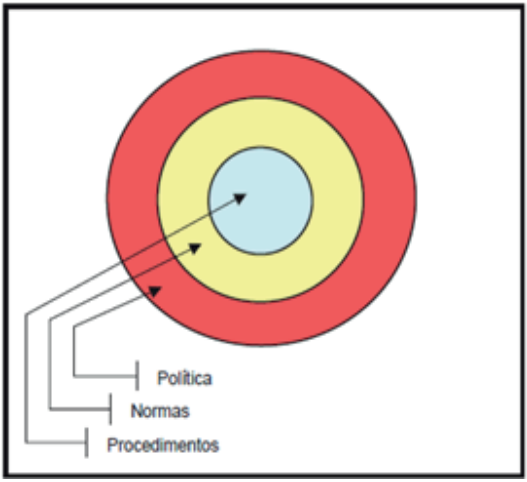

Fig. 1 - Estrutura da PSI

5. REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.1. Proteção da Informação (Ref.: ISO 27001 e 27002)

A informação é um importante ativo para a execução das atividades operacionais e assistenciais e para manter a qualidade e perenidade do plano de saúde. Tal como os ativos da FUNDAFFEMG, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, documentos digitais e/ou digitalizados, documentos impressos ou manuscritos, microfilmes, e-mails, e até mesmo por meio da comunicação oral.

Toda informação relacionada às operações da FUNDAFFEMG, gerada ou desenvolvida nas dependências da FUNDAFFEMG ou por operador durante a execução das atividades de tratamento da informação no país ou fora dele, desde que o país estrangeiro firme contrato de observância à legislação brasileira, para a FUNDAFFEMG, ou ainda gerada e/ou tratada por prestadores de serviços no exercício das atividades contratadas, constitui ativo desta instituição, essencial à condução de suas atividades, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da FUNDAFFEMG e estará sujeita aos sansões previstas no Código de Ética da FUNDAFFEMG.

É diretriz que toda informação de propriedade da FUNDAFFEMG esteja sujeita à Política de Gestão de Riscos estabelecida e Relatório de Impacto RIP, nos termos da Lei 13.709/2018, sob monitoramento constante dos riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

5.2. Responsabilidades

É missão e responsabilidade de cada agente de tratamento que mantém relação de negócio, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas em nome do Controlador, seja por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

Para auxiliar a todos os colaboradores nessa missão, a FUNDAFFEMG designará o Encarregado conforme preconiza o inciso VIII do art. 5º da Lei 13.709/2018.

5.3. Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, prontuários, exames, laudos assistenciais, exames, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela FUNDAFFEMG e/ou obtidas por meio do exercício do trabalho no tratamento da informação, em decorrência da execução do contrato de trabalho ou de prestação de serviços firmado com a FUNDAFFEMG.

São responsáveis pela observância desta Política os conselheiros, diretores, empregados, prestadores de serviço, agentes de tratamento e consultores (incluindo advogados, auditores e técnicos especializados) dos controladores.

O operador que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem consentimento por escrito e/ou autenticado pelo responsável legal da FUNDAFFEMG. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pela FUNDAFFEMG. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades de negócio da FUNDAFFEMG.

O agente de tratamento deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.

O operador deverá informar prontamente ao Encarregado da FUNDAFFEMG sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política: (i) o atendimento a quaisquer determinações decorrentes de lei ou emanada do Poder Judiciário ou Legislativo, tribunais arbitrais e de órgãos públicos administrativos; (si) a divulgação das informações confidenciais aos agentes, representantes (incluindo, mas não se limitando, a advogados, auditores e Consultores técnicos) e empregados das partes; e, (iii) as informações confidenciais que forem divulgadas após o consentimento, por escrito, da FUNDAFFEMG.

Se a qualquer uma das partes ou seus representantes legais, que detém as informações confidenciais, for solicitado ou requerido, oralmente ou por escrito, solicitações de informações de documentos, mandados de investigações civis ou qualquer outro pedido similar, para revelar tais informações confidenciais, deverá notificar prontamente a outra parte para que esta tenha tempo hábil para verificação, inclusive, se for o caso, aplicar as ressalvas contidas nos termos desta Política.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o operador

e/ou parceiro controlador de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

5.4. Violação da Política, Normas e Procedimentos de Segurança da Informação
As violações de segurança devem ser informadas ao Comitê de Segurança da Informação, por meio do Encarregado. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:
• uso ilegal de software;
• introdução (intencional ou não) de vírus de informática;
• tentativas de acesso não autorizado a dados e sistemas;
• compartilhamento de informações sensíveis do negócio;
• divulgação de informações dos titulares dos dados e das operações contratadas.

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração da FUNDAFFEMG e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os operadores às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir, aos sansões previstas no Código de Conduta Ética, podendo alcançar a rescisão de contratos como resultante de processo administrativo disciplinar.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, o agente de tratamento deve entrar em contato com Encarregado designado pela Diretoria Executiva.

6. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

6.1. Classificação da Informação

De acordo com a ISO 27001, a classificação da informação tem o objetivo de assegurar o nível adequado de proteção para a informação. A classificação tem como base o seu valor, criticidade para a organização e requisitos legais. A boa prática diz que a classificação deve ser feita de acordo com o seguinte processo:

6.2. Inventário de ativos (Registro de ativo)

O propósito é saber quais informações classificadas, a FUNDAFFEMG tem em sua posse, e quem é responsável por elas (ou sejam seu proprietário).

Informação classificada pode estar em diferentes formatos e tipos de mídia, como por exemplo:

- Documentos eletrônicos;
- Sistemas de informação / bases de dados;
- Documentos em papel;
- Mídias de armazenamento (ex.: pendrives, discos, cartões de memória, etc.);
- Informação transmitida verbalmente;
- E-mail.

Esta política define quatro grandes blocos de classificação, sem prejuízo de complementação posterior por meio de norma específica; sendo: três níveis de confidencialidade e um nível público:

- Confidencial (o mais alto nível de confidencialidade);
- Restrita (médio nível de confidencialidade);
- Uso interno (o mais baixo nível de confidencialidade);
- Pública (todos podem ver a informação).

O proprietário do ativo é o responsável por classificar a informação, quanto maior o valor da informação (quanto maiores as consequências de uma quebra da confidencialidade), maior deve ser o nível de classificação

6.3. Rotulagem da informação

Após a classificação da informação, a FUNDAFFEMG, por meio de norma específica irá definir os critérios de rotulagem (atribuição do grau de confidencialidade) baseado em nível de confidencialidade;

6.4. Manuseio de ativos

O manuseio de ativos (informação) resultante do inventário de ativos observará a classificação a ser definida em norma específica conforme critérios dispostos no quadro abaixo e fica sujeito às regras de controle de acesso definido pelo proprietário da informação (gestor da unidade).

	Uso interno	Restrito	Confidencial	Público
Documentos eletrônicos				
Sistemas de informação				
Documentos em papel				
Mídia de armazenamento				
Informação transmitida verbalmente				
E-mail				
WhatsApp				
Redes Sociais				
Jornais e Boletins				

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas por: regras de controle de acesso/ segregação de funções e/ou Termo de sigilo, de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário. Cabe ao agente de tratamento todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, processos administrativos instaurados pela reguladora, processos judiciais, perdas de produtividade ou imagem da FUNDAFFEMG, podendo levar à extinção das operações ou prejuízos graves à credibilidade e crescimento.

São exemplos de informações confidenciais:

• Informações de beneficiários que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG, etc.), situação clínica, informações de credo, orientação sexual, etc.);

• Informações sobre acordos contratuais que revelem vantagens competitivas da FUNDAFFEMG frente ao mercado;

• Todo o material estratégico da FUNDAFFEMG (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);

• Quaisquer informações da FUNDAFFEMG, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
• Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidade. Estas informações são também pessoais e intransferíveis.

6.5 Acesso a Sistemas e Recursos de Rede
O operador, em nome do Controlador, é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.

A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Periodicamente, os acessos concedidos devem ser revistos pelo gestor da unidade e/ou encarregado.

6.6.Utilização dos Recursos de Informação
Apenas os equipamentos e softwares disponibilizados e/ou homologados pela FUNDAFFEMG podem ser instalados e conectados à rede da FUNDAFFEMG.

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

6.7. Autenticação e Senha
O operador é responsável por todos os atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os operadores da informação devem:

• Manter a confidencialidade, memorizar e não registrar a senha em lugar algum. Ou seja, não a informar a ninguém e não anotá-la em papel; ou em qualquer meio eletrônico;
• Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
• Selecionar senhas de qualidade, que sejam de difícil adivinhação;
• Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
• Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del). Não aguardar bloqueio automático

6.8. Direito de Acesso (Autorização)
O operador é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que lhe são conferidos. O gestor da unidade é a autoridade competente para solicitação de acesso controlado aos sistemas e documentos de seus funcionários, estagiários, prestadores de serviços, parceiros e visitantes, sendo intransferíveis.

A solicitação de acesso à informação deve decorrer da necessidade funcional do operador de dados.

6.9. Direitos de Propriedade
Todo produto resultante do trabalho dos agentes de tratamento da informação (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da FUNDAFFEMG. Em caso de extinção ou rescisão do contrato de trabalho ou prestação de serviços, por qualquer motivo, deverá o agente de tratamento devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços à FUNDAFFEMG, ou emitir declaração de que as destruiu.

6.10. Equipamentos particulares/privados
Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Organização.

Casos especiais, expressamente autorizados pela Diretoria Executiva da Fundação, serão respaldados por Termo de responsabilidade específico para essa finalidade.

6.11. Home Office
O acesso remoto aos sistemas e computadores da FUNDAFFEMG, serão submetidos à norma específica emitida pela unidade de Tecnologia e Informação e restrito aos trabalhadores autorizados formal e expressamente para esse regime laboral.

O manuseio de documentos impressos por funcionário em regime de Home Office será lastreado em termo de sigilo entre a FUNDAFFEMG e funcionário e deve observar todos os critérios de confidencialidade desta política e normas especificas subsequentes.

6.12. Mesa Limpa e Tela Limpa (ISO 27001 e 27002)
Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. A utilização da área de trabalho nas telas de computador para acesso rápido a dados pessoais e sensíveis também deve ser inibida, assim como notas adesivas eletrônicas contendo informações protegidas pela LGPD ou relativas ao negócio da Fundaffemg. Lixeiras físicas ou eletrônicas devem ser esvaziadas diariamente.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente. Os dados e documentos que ficam armazenados na memória das impressoras devem ser descartados sistematicamente e observada a norma específica exarada da Unidade de Tecnologia e Informação.

6.13. Conversas em Locais Públicos e registro de informações
Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas à FUNDAFFEMG.

6.14. Leis e Regulamentos
É de responsabilidade do operador, em nome do Controlador, conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

6.15. Aspectos de Disseminação da Política
A política e as Normas de Segurança da Informação na FUNDAFFEMG devem ser amplamente divulgadas entre os seus colaboradores, por todas as mídias de comunicação interna, devendo estar disponível para acesso em rede interna acessível a qualquer momento.

7. RESPONSABILIDADES

7.1. Encarregado da FUNDAFFEMG
A Diretoria Executiva, designará do Encarregado nos termos da Lei Geral de Proteção de Dados.

Cabe Encarregado

• Avaliar ajustes, aprimoramentos e modificações desta Política;
• Avaliar melhorias e Normas de Segurança da Informação conjuntamente com a unidade de Tecnologia da Informação;
• Submeter a aprovação da Diretoria Executiva as propostas de melhorias e normas de segurança da Informação;
• Avaliar a classificação das informações pertencentes ou sob a guarda da FUNDAFFEMG, com base no inventário de informações e nos critérios de classificação constantes de norma específica com apoio da unidade de tecnologia e informação;
• Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando relatório de análise conclusiva à Diretoria Executiva, para julgamento, quando for o caso;
• Avaliar projetos e iniciativas relacionados à melhoria da segurança da informação da FUNDAFFEMG;
• Avaliar o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
• Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
• Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

• Avaliar os trabalhos de análise de vulnerabilidade realizados pela área de Gestão de Segurança da Informação do Gestor de Informática e/ou empresa especializada parceira, quando couber;
• Submeter os relatórios sistemáticos de avaliação aos membros do 1º escalão da instituição, para avaliação e tomada de decisão;
• Outras atribuições que venha julgar relevante para o interesse e garantia da segurança das informações da FUNDAFFEMG.

7.2. Diretoria Executiva
Em relação à segurança da informação, cabe à Diretoria da FUNDAFFEMG:

• Aprovar a Política de Segurança da Informação e suas revisões;
• Tomar as decisões administrativas referentes aos casos de descumprimento da política e/ou de suas Normas encaminhados pelo Comitê.

7.3. Área de Gestão de Segurança da Informação

7.3.1. Encarregado
É de responsabilidade do Encarregado:

• Convocar, coordenar, lavrar atas e prover relatórios gerenciais à Diretoria Executiva;
• Prover todas as informações de gestão de segurança da informação solicitadas pela Diretoria Executiva;
• Oferecer orientação sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores da FUNDAFFEMG;
• Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação para a FUNDAFFEMG com apoio da unidade de Tecnologia e Informação, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
• Analisar os riscos relacionados à segurança da informação da FUNDAFFEMG e apresentar relatórios periódicos sobre tais riscos a Diretoria Executiva, acompanhados de proposta de aperfeiçoamento do ambiente de controle da segurança, quando for o caso;
• Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da FUNDAFFEMG;
• Requisitar informações às demais áreas da FUNDAFFEMG (diretorias, superintendentes, gestores etc.), realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação;

• Implantar procedimento para ativar e manter registros de vulnerabilidades e ataques reportados por fontes confiáveis, além de medidas de controle e correção, promovendo-se, quando necessário, as devidas orientações de intervenção aos administradores dos recursos vulneráveis; e
• Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação.

7.3.2. Gestor da Unidade de Tecnologia e Informação
• Estabelecer procedimentos e realizar a gestão dos sistemas da FUNDAFFEMG, bem como do seu controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
• Manter o plano de continuidade dos serviços essenciais de Tecnologia da Informação;
• Garantir a realização do backup dos dados de serviços essenciais da instituição, de acordo com a periodicidade previamente definida e aprovada pelo Comitê de Segurança da Informação;
• Assegurar o controle de tráfego de dados entre os computadores da rede interna e rede externa de forma a prevenir ataques e vazamento de dados sensíveis.
• Disponibilizar redundância dos serviços essenciais para minimizar o tempo de interrupção da operação.

7.3.3. Administrador de Sistema / Operações
Assegurar mecanismos restritivos a que usuários do sistema não autorizados tenham acesso a informações confidenciais;
• Adequar os sistemas computacionais e de comunicação em conformidade com a Política de Segurança.

7.4. Proprietário da Informação
O proprietário da informação é o responsável pela autorização do acesso a ela.
Na FUNDAFFEMG, os gestores de unidade determinam quais serão os acessos concedidos e em que níveis, neste contexto são responsáveis pelas respectivas unidades de negócio da organização, as quais podem ser diretamente afetadas caso alguma informação torne-se pública, corrompida ou perdida.

No caso de arquivamento de documentação física dentro da sede, o gestor da unidade de arquivamento é responsável pelo controle de acesso devendo monitorar a guarda e eventuais disponibilizações a outras unidades por meio de registro eletrônico ou físico;

No caso de arquivamento de documentação física por meio de empresa especializada contratada o controle de acesso, disponibilização e devolução de documentos fica sob a responsabilidade da unidade de operações.

Cabe ao proprietário da informação:

• Elaborar, para toda informação sob sua responsabilidade, matriz ou planilha que relacione cargos e funções às autorizações de acesso concedidas;
• Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz ou planilha de cargos e funções, a Política e as Normas de Segurança da Informação da FUNDAFFEMG;
• Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
• Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
• Analisar os relatórios de controle de acesso a sistemas corporativos fornecidos pela unidade de TI, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
• Fornecer todas as informações e documentos solicitados em caso de investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
• Participar, sempre que convocado, das reuniões do COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO DA FUNDAFFEMG, prestando os esclarecimentos solicitados.

7.5. Assessoria da Diretoria/Jurídica
Cabe à Assessoria Jurídica:

• Manter as áreas da FUNDAFFEMG informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
• Atualizar os acordos entre os Controladores: aspectos legais de uso intencional e requisitos de segurança;
• Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da FUNDAFFEMG;
• Avaliar, quando solicitados, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da FUNDAFFEMG quanto a seus aspectos legais; e
• Tomar as providências jurídicas cabíveis em casos de incidentes de segurança.

7.6. Superintendentes e Gestores
Cabe aos Superintendentes e Gestores:

• Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
• Assegurar que suas equipes possuam acesso e conhecimento da Política, das Normas e dos Procedimentos de Segurança da Informação;
• Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados;
• Comunicar imediatamente eventuais casos de violação de segurança da informação ao Encarregado

7.7. Área de Recursos Humanos
Cabe à área de Recursos Humanos:

• Manter atualizado o Código de Conduta Ética da FUNDAFFEMG especialmente quanto aos requisitos de sigilo e sanções disciplinares em caso de descumprimento desta política, assim como propor normas especificas que disciplinem a matéria;
• Elaborar aditamento aos contratos de trabalho dos funcionários e estagiários, quando necessário, adequando à legislação de proteção de dados, arquivando-o nas respectivas pastas;
• Elaborar contrato de trabalho adequado à legislação de proteção de dados para os ingressos;
• Informar aos ingressos sobre a Política, Normas e Procedimentos de Segurança da Informação adotados pela FUNDAFFEMG;
• Elaborar e aplicar, sob a orientação do Encarregado, treinamento sobre Segurança da Informação na Fundação, sempre que necessário;
• Informar, prontamente, ao Encarregado e unidade de Tecnologia da Informação, todos os desligamentos, afastamentos e modificações no quadro funcional da Fundação;
• Tomar as providências administrativas no caso de aplicação de penalidades aos funcionários e quanto ao não cumprimento da Política de Segurança da Informação.

7.8. Geral
Cabe a todos os usuários da rede da FUNDAFFEMG:

• Tomar conhecimento dessa política;
• Seguir todas as ações de acordo com essa política;
• Informar à segurança qualquer violação conhecida a essa política;
• Informar à segurança qualquer suspeita de problemas com essa política;
• Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área

7.9. Operadores

a) Funcionário:

Acesso a máquinas especificamente autorizadas na forma em que encontra especificamente autorizada;

Solicitar autorização prévia por escrito ao gestor da unidade para qualquer ação que possa ser interpretada como uma questão de segurança.

b) Contratado ou convidado (Nesta categoria incluem-se auditores externos, analistas e técnicos contratados, visitantes, pacientes e outros):

7.9.1.Nenhum acesso a recursos de computação, a menos que haja notificação prévia por escrito à segurança e autorização expressa da mesma.

8. PENALIDADES

A não observância dos preceitos desta Política poderá implicar na aplicação de sanções administrativas previstas no Código de Conduta Ética, normas especificas que disciplinem a matéria, contrato de trabalho firmado com a FUNDAFFEMG, assim como sanções cíveis e penais previstas na legislação em vigor que regule ou venha regular a matéria.

As penalidades administrativas serão aplicadas após a sua devida apuração em processo administrativo disciplinar, sendo observados critérios de gravidade e reincidência dos atos de violação cometidos à Política de Segurança da Informação.

As infrações ocorridas violando as normas que compõem a Política de Segurança da Informação deverão ser analisadas pelo gestor imediato do infrator, que deverá comunicar imediatamente ao Encarregado para fins de determinação da apuração das eventuais responsabilidades dos funcionários envolvidos.

9. REFERÊNCIAS BIBLIOGRÁFICAS

ANS NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES - PROCESSO Nº: 33910.029786/2019-51

GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) - Comitê Central de Governança de Dados - Administração Pública Federal – Abril/2020

https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf

ISO 27001 – Sistema de Gestão de Segurança da Informação;
ISO 27002 – Controles de Segurança da Informação;
ISO 38500 – Governança de TI;
ISO 31000 – Gestão de Riscos;
ISO 27005 – Gestão de Riscos de Segurança da Informação e;
COBIT - Control Objectives for Information and related Technology.
Artigo Serpro e LGPD – Segurança e inovação – Carla Freitas

RESOLUÇÃO Nº 02/2021 DA DIRETORIA EXECUTIVA DA FUNDAÇÃO AFFEMG DE ASSISTÊNCIA E SAÚDE – FUNDAFFEMG DE 14 DE JANEIRO DE 2021

Aprova Política de Segurança da Informação e dissolve a Comissão criada pela Portaria 02/2020.

A Diretoria Executiva da Fundação AFFEMG de Assistência e Saúde - FUNDAFFEMG, vista do que dispõe o artigo 28 do Estatuto:

RESOLVE:

Art. 1° - Aprovar Política de Segurança da Informação, versão 01, elaborada pela Comissão designa por meio da Portaria Nº 002/2020 de 25 de agosto de 2020.

Art. 2° - Neste ato, fica dissolvida a Comissão criada pela Portaria 02/2020 e a Diretoria Executiva designará o Encarregado da FUNDAFFEMG nos termos do inciso VIII do Art. 5° da Lei 13.709 de 14 de agosto de 2018 alterada pela Lei 13.853/19.

Art. 9° Esta Resolução Administrativa entra em vigor na data de sua assinatura digital.

MUNIR NACIF MITRE:05632072649 Assinado de forma digital por MUNIR NACIF MITRE:05632072649 Dados: 2021.01.21 13:16:11 -03'00'

Munir Nacif Mitre
Diretor Presidente

ANTONIO CAETANO JACINTO LEMOS:27765849620 Assinado de forma digital por ANTONIO CAETANO JACINTO LEMOS:27765849620 Dados: 2021.01.21 13:19:54 -03'00'

Antonio Caetano Jacinto Lemos
Diretor de Assistência à Saúde

LUIZ ANTONIO RIBEIRO:27744043634 Assinado de forma digital por LUIZ ANTONIO RIBEIRO:27744043634 Dados: 2021.01.21 13:18:24 -03'00'

Luiz Antonio Ribeiro
Diretor Administrativo e Financeiro

ANS nº 31556-7

FUNDAFFEMG

NOSSO PLANO É VIDA E SAÚDE

Rua Sergipe, 893 - Savassi - CEP 30130 171 - BH - MG
Telefone: 31 2103 5858 - www.fundaffemg.com.br