Tipo de Documento: **POLÍTICA**	Setor: **CONTROLE INTERNO E OUVIDORIA**		Responsável pela validação: **Taís Raquel de Oliveira Santana**	
Técnico Elaborador: **Maria Gabrielly Sales Vitoriano Uchôa**	Versão: **01**	Data: **MAIO/2024**	Código: **P-004/2024**	Data Validação: **10/06/2024**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

APRESENTAÇÃO

As Políticas Institucionais da Fundação de Apoio à Gestão Integrada em Saúde de Fortaleza - FAGIFOR são expressões dos parâmetros e intenções da alta gestão, coerentes com os valores éticos e as ferramentas estratégicas de Missão, Visão e Valores que ajudam a direcionar a instituição ao seu objetivo.

Considerando a sensibilidade do tema, o presente documento trata da Política de Segurança da Informação, indicando procedimentos e abordando conceitos, a fim de tratar sobre regras práticas e responsabilidades de empregados públicos, servidores, colaboradores e outros interessados desta Fundação, com o extremo cuidado e a máxima confidencialidade.

Assim, esta Política pode ser utilizada para promover uma cultura de privacidade e conscientização das pessoas para minimizar os riscos e explicar como a Fundação age em relação ao tema.

1. OBJETIVOS

Esta Política tem como objetivo tratar da segurança da informação, no sentido de minimizar riscos, bem como orientar os empregados públicos, colaboradores e terceiros interessados desta Fundação acerca das diretrizes aplicáveis, com base nas legislações vigentes.

Aqui, será tratado sobre a proteção das informações, garantindo que sejam atendidas às normas brasileiras e internacionais ao mesmo tempo, com o intuito de garantir:

a) a participação e o cumprimento por todos os colaboradores;

b) o compromisso da Fundação em proteger as informações de sua propriedade e/ou sob sua guarda;

c) a confiabilidade das informações por meio da preservação da integridade, da confidencialidade e da disponibilidade dos dados desta Fundação.

Este documento possibilita o gerenciamento da segurança da informação nesta Fundação, estabelecendo regras e padrões para proteção da informação e possibilita manter a confidencialidade, garantindo que a informação não seja alterada ou perdida, permitindo a disponibilidade quando for necessário.

É imprescindível a adoção de condutas, normas e procedimentos padronizados que tenham como objetivo garantir a proteção dos três princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Para isto, são objetivos desta Política:

a) Proteger a informação, de forma a garantir sua confiabilidade, autenticidade e integridade;

b) Estabelecer diretrizes para a utilização dos recursos de informação, serviços de redes de dados, estações de trabalho, Internet, telecomunicações, correio eletrônico e outros;

c) Designar papeis e responsabilidades relativas à segurança da informação nesta Fundação;

d) Ser transparente e inclusiva, de forma a conscientizar todos os empregados da Fagifor sobre a importância das informações e de suas vulnerabilidades;

e) Promover e desenvolver a cultura de segurança da informação em todos os níveis da Fundação;

f) Ser parte integrante dos processos organizacionais;

g) Possibilitar a criação de controles e promover a otimização dos recursos de tecnologia da informação.

Além disso, serão abordadas as diretrizes e responsabilidades que assegurem e reforcem o compromisso da Fagifor com o cumprimento das legislações de proteção de dados.

2. DIRETRIZES

As diretrizes são:

a) confirmar a integridade, confiabilidade e autenticidade dos dados;

b) garantir a proteção e guarda das informações;

c) utilizar recursos de informação para garantir o desempenho das atividades da Fagifor;

d) classificar as informações com o objetivo de identificar o nível de proteção;

e) estabelecer regras e procedimentos;

f) prevenir possíveis causas de incidentes;

g) segurança física;

h) capacitação e aperfeiçoamento dos colaboradores;

i) pessoalidade do acesso.

3. APLICAÇÃO

Esta política é aplicável aos empregados públicos, colaboradores e outros interessados/terceiros desta Fundação.

4. DEFINIÇÕES E CONCEITOS

a) Dados Pessoais: são todas as informações que identifiquem um(a) cidadão(ã) ou que permita sua identificação. Exemplo: nome, CPF, telefone, entre outros.

b) Dados Sensíveis: são informações referentes à origem racial ou étnica, religião, opinião política, dado referente à saúde ou à vida sexual, entre outros.

c) Lei Geral de Proteção de Dados: Lei Federal nº 13.709, de 14 de agosto de 2018, acerca do tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo como objetivo defender os titulares de dados pessoais e ao mesmo tempo permitir o uso dos dados para finalidades diversas, equilibrando interesses e

harmonizando a proteção da pessoa humana com o desenvolvimento tecnológico e econômico.

d) Terceiros/Interessados: são todas as pessoas físicas e/ou jurídicas que a Fundação se relaciona ou irá se relacionar, para desenvolver ou auxiliar no desenvolvimento das suas atividades. Exemplo: prestador de serviço, fornecedor, entre outros.

e) Titular de Dados: pessoa natural (física) a quem se referem os dados pessoais.

f) Tratamento de Dados Pessoais: qualquer operação realizada com os Dados Pessoais do Titular de Dados. Exemplo: eliminação, recepção, classificação, utilização, acesso, entre outros.

g) Norma ISO 27001: é o padrão e referência Internacional para a gestão de segurança da informação.

h) Confidencialidade: é um termo que diz respeito a manter informações em sigilo, protegendo os dados.

i) Informação: dados estruturados, organizados e processados, apresentados dentro do contexto, que o torna relevante para quem o deseja obter.

j) Incidente: qualquer acontecimento confirmado ou sob suspeita, relacionado à segurança dos sistemas, das informações ou das redes de computadores.

l) Classificação da informação: consiste na definição de níveis de proteção que cada dado deve receber, identificando e definindo níveis e critérios adequados para a proteção das informações, de acordo com sua importância para as organizações.

m) Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

n) Utilização dos recursos da informação: os recursos disponibilizados são fornecidos com o objetivo único de garantir o desempenho das atividades da FAGIFOR. O acesso e o uso da informação e dos recursos de tecnologia da informação devem ser controlados e limitados para o cumprimento das atividades de cada usuário.

o) Segurança física: controles que monitoram o acesso físico a equipamentos, documentos, suprimentos e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso.

p) Capacitação e aperfeiçoamento: é o processo permanente e deliberado de aprendizagem, utilizando práticas para promover as habilidades. Os colaboradores deverão se capacitar continuamente para o desenvolvimento de competências em segurança da informação.

q) Pessoalidade de acesso: é a identificação do colaborador, pessoal e intransferível, que permita de maneira clara o seu reconhecimento, para ter acesso às informações, sistemas e dependências de responsabilidade da Fagifor.

5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A presente Política foi desenvolvida para registrar o compromisso da FAGIFOR para estabelecer a forma de tratamento das informações de empregados públicos, colaboradores e terceiros/interessados, com o máximo cuidado e confidencialidade necessária.

Com isto, garantimos que atendemos aos ditames da Lei Geral de Proteção Dados (LGPD), Lei Federal de número 13.709/2018, que assegura o direito à privacidade e à proteção de dados pessoais de usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais.

Ao tratar de um ambiente altamente volátil quanto às transformações tecnológicas e de informação, é necessário fomentar a cultura de proteção à privacidade, aos dados pessoais e aos dados em geral.

Todos os dados coletados pela FAGIFOR serão tratados como confidenciais e utilizados para os fins descritos e, quando for o caso, autorizados pelo empregado público, colaborador e terceiro/interessado. Importante frisar que todos que tratam dados pessoais são responsáveis por sua proteção, inclusive o próprio titular.

Serão tratados três pontos que merecem destaque nesta Política, quais sejam:

a) Uso de aplicativos de mensagens: uso seguro de aplicativos de mensagens na comunicação interna da Fagifor, inclusive com terceiros, visando proteger informações sensíveis e cumprir a LGPD. Sobre esse ponto, faz-se necessário destacar dois pontos:

- Evitar o compartilhamento de informações sensíveis, como dados pessoais, informações de saúde e dados financeiros, através de aplicativos de mensagens.
- Para comunicações internas e externas, deverá ser evitado o uso de aplicativos de mensagens para informações sensíveis, preferindo-se o uso de e-mails institucionais e/ou plataformas internas seguras.

b) Descarte Seguro de Documentos Físicos: visa proteger informações sensíveis em cumprimento à LGPD. Garantirá que qualquer informação sensível seja destruída de forma irreversível, impedindo que dados pessoais ou confidenciais sejam recuperados ou utilizados de maneira inadequada. A destruição de documentos deverá ser realizada por meio de métodos seguros, como fragmentação ou incineração, e todos os colaboradores devem ser instruídos sobre a importância do descarte seguro e os procedimentos a serem seguidos. Nesse contexto, é oportuno o seguinte destaque:

- Para assegurar a conformidade, a Fagifor estabelecerá pontos de coleta seguros para documentos a serem descartados, onde somente pessoal autorizado tenha acesso. Além disso, deverão ser realizadas auditorias periódicas para verificar a eficácia dos procedimentos de descarte e garantir que todas as etapas estejam sendo seguidas corretamente.

c) Política de Compartilhamento de Arquivos: arquivos que contenham informações sensíveis ou confidenciais devem ser, preferencialmente, compartilhados utilizando e-mail do “Google ou Google drive”. Além disso, é fundamental assegurar que os compartilhamentos, enquanto utilizados pela plataforma Gmail não restrita, nos casos de desligamento de um funcionário, o gestor imediato irá rever os compartilhamentos no Google drive, retirando os compartilhamentos, garantindo assim o não acesso a partir da data do desligamento. Os e-mails institucionais criados no Gmail com *“.fagifor”*, obrigatoriamente deverão ter o e-mail de recuperação do gestor da GETIC. Assim, será garantido que mesmo após a saída do funcionário, a Fagifor tenha acesso aos conteúdos.

Esta Fundação, em relação à Segurança da Informação, obedece aos seguintes princípios:

a) Finalidade: é realizado o tratamento dos dados pessoais para propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior de forma incompatível com as finalidades que foram apresentadas ou em desacordo com o que foi informado.

b) Adequação: é realizado o tratamento de dados pessoais de forma compatível com as finalidades informadas ao titular de dados e de acordo com o contexto.

c) Necessidade: o tratamento de dados pessoais realizado será limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos

dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

d) Livre acesso: consulta facilitada com relação ao uso dos dados pessoais, prestando informações claras e acessíveis.

e) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis, de acordo com a necessidade e para o cumprimento da finalidade.

f) Segurança: garante a utilização de medidas técnicas e administrativas adequadas ao tratamento e proteção de dados pessoais quanto aos acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão

g) Medidas de Prevenção: é garantido a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de seus dados pessoais.

h) Não discriminação: diz respeito à proibição do tratamento para fins discriminatórios ilícitos ou abusivos.

i) Responsabilização e prestação de contas: deverá ser demonstrada as providências necessárias e medidas eficazes para o cumprimento das normas de proteção de dados pessoais.

Os dados do empregado público, colaborador e terceiro/interessado serão tratados com confidencialidade, dentro dos limites legais e de acordo com esta Política. Todos os esforços serão utilizados para garantir a segurança de proteção de dados coletados de qualquer forma de tratamento inadequado ou ilícito, como:

a) Recursos de navegação segura;
b) Informações, sempre que possível, criptografadas;
c) Restrição de acesso a informações pessoais por parte de funcionários e de pessoal não autorizado;

d) Medidas de segurança física para que não ocorra acesso indevido aos sistemas e infraestrutura.

Eventualmente, poderá ser utilizado os dados para finalidades não previstas nesta Política, mas que estejam dentro das normas legais. Quando não cumprir essa prerrogativa, será feito mediante autorização.

Ressalta-se que nenhum sistema é completamente seguro. Assim, caso haja suspeita de dados em risco, é importante o contato imediato com a Gerencia de Tecnologia da Informação e Comunicação.

6. RESPONSABILIDADES

No contexto desta Política, todos os usuários são encorajados a considerar cuidadosamente as ações que venham a tomar e a entrar em contato com a FAGIFOR caso tenham alguma dúvida, preocupação ou sugestões relacionadas a temática.

O usuário é responsável por todos os atos praticados com suas identificações, dentre as quais, exemplificamos: nome do usuário na rede, carimbo, crachá, endereço de endereço eletrônico e assinatura digital. É responsável por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, ficam sujeitos a sanções previstas no Código de Conduta, Ética e Integridade, bem como seu Manual de Correição e normas de proteção de dados, bem como Código Civil e

Código Penal e Processo Penal, desde que seja garantida a ampla defesa e contraditório.

Esta Política, em relação às responsabilidades e em conformidade com as normas de proteção de dados pessoais, deverá, entre outros:

a) fornecer treinamentos aos colaboradores;
b) revisar processos para diminuição dos riscos que envolvem o tratamento de dados pessoais;
c) investir em ferramentas de gestão e governança de dados pessoais;
d) investir em ferramentas tecnológicas de segurança da informação, que permeiam todo o ciclo de vida do dado;
e) orientar, liderar e dar suporte para a prevenção de incidentes;
f) estabelecer e aprimorar programas e sistemas para prevenção de incidentes de segurança da informação;
g) monitorar sistemas de segurança.

Além disso, é responsabilidade da área gestora garantir a divulgação da Política para a equipe, cujo conteúdo deverá nortear a elaboração de instrumentos normativos, manuais e instruções de trabalho.

Assim, todos têm responsabilidade para garantir a Segurança da Informação.

7. DESCUMPRIMENTO DA POLÍTICA

O descumprimento desta Política pode resultar em ações corretivas apropriadas, levando em consideração a gravidade da não conformidade.

8. REVISÃO E MELHORIA CONTÍNUA

Esta Política entra em vigor na data de sua aprovação pelo Conselho Curador, sendo prevista sua revisão e eventual alteração em até 12 meses, devendo novamente ser objeto de deliberação para validação pelo mesmo Conselho da aprovação inicial.

A FAGIFOR assume como compromisso institucional a avaliação periódica das finalidades de suas operações de tratamento, considerando o contexto em que estas operações se inserem, os riscos e benefícios que podem ser gerados.

Esta Política poderá ser alterada a qualquer tempo, caso haja necessidade.

9. DISPOSIÇÕES GERAIS

Esta Política poderá ser utilizada para promover uma cultura de privacidade e conscientização das pessoas para a proteção de dados e como será gerenciado os incidentes, caso haja.

O uso dos conceitos previstos neste documento poderá ser utilizado sempre que tiver dúvidas quanto ao tratamento dos seus dados pessoais. Importante destacar que todos que tratam de dados pessoais são responsáveis por sua proteção, inclusive o próprio titular.

Será garantida a disponibilização da referida política no sistema de gestão de documentos, juntamente com sua inclusão nos materiais de capacitação permanente dos colaboradores e gestores da FAGIFOR.

A área gestora deverá também promover, em articulação com a área de gestão de pessoas, o treinamento das equipes de trabalho, de modo a assegurar que todos tenham conhecimento e o comprometimento ao cumprimento dos normativos estabelecidos pela Fundação.

10. REFERÊNCIAS

A presente Política se baseia nas seguintes normas:

a) Lei Geral de Proteção de Dados - LGPD - Lei nº 13.709, de 14 de agosto de 2018;

b) Alteração da LGPD - Lei nº 13.853, de 08 de julho de 2019;

c) Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014;

d) Lei de Acesso à Informação - Lei nº 12.527, de 18 de novembro de 2011;

e) Decreto nº 13.305 de 21 de fevereiro de 2014 – Dispõe sobre específicas para a implementação da Lei de Acesso à Informação no âmbito do Poder Executivo Municipal;

f) Instrução Normativa GSIPR nº 01/2008, que dispõe sobre as orientações que deverão ser implementadas na Gestão de Segurança da Informação pelos órgãos e entidades da Administração Pública Federal;

g) Decreto Federal nº 9.637, de 26 de dezembro de 2018;

h) Norma Complementar nº 03/IN01/DSIC/GSIPR, que institui diretrizes para a elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

i) Lei Federal nº 12.527/2011, que dispõe sobre o acesso a informações no âmbito do setor público;

j) Decreto Federal nº 7.845/2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo;

k) Norma ISO 27001 - Sistema de Gestão da Segurança da Informação;

l) Norma ISO 27002 - Controles de Segurança da Informação;

m) Código de Conduta, Ética e Integridade da Fagifor.