Área:	1. DIRETORIA PRESIDÊNCIA - DP
	CARGO
Elaboração	ASSESSOR (A)
Revisão	ASSESSOR (A), CHEFE DO NÚCLEO DE QUALIDADE
Aprovação	CHEFE DO NÚCLEO DE QUALIDADE

CO-AUTOR(ES)

1.INTRODUÇÃO:

Esta Política foi elaborada com o intuito de orientar e implementar diretrizes de Segurança da Informação no Instituto de Gestão Estratégica de Saúde – IgesDF, utilizando como base a NBR ISO IEC 27002, NBR ISO IEC 27001, NBR ISO IEC15408, ISO IEC PSTR18044, NBRISO13335,NBR ISO 11514, NBR ISO 11515, NBR ISO 11584, BS 7799, do British Standard Institute, na reforma do BürgerlichesGesetzbuch (BGB) envolvendo documentos eletrônicos, no Data ProtectionWorkingParty , da União Européia, no Statuto dei LavoratoriItaliani, CodicedellaPrivacy(Itália), Diretiva 2002/58/CE; Decreto Legislativo Italiano n.º 196 de 30 de junho de 2003 (MisurediSicurezza), (normativas ou decretos).

2.OBJETIVOS:

Este documento tem como objetivo orientar ações, procedimentos e diretrizes para o uso dos ativos de Informação do Instituto de Gestão Estratégica de Saúde – IgesDF, ou a ele confiados, com o intuito de garantir a confidencialidade, integridade, disponibilidade e privacidade das informações, sendo aplicável a todos os nossos colaboradores. Além de estabelecer diretrizes em relação à manipulação de informações e utilização da infraestrutura tecnológica do IgesDF, de acordo com princípios éticos e legais. Este documento tem por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades, e criar uma cultura educativa governamental de segurança da informação e proteção aos dados no IgesDF.

3.DEFINIÇÕES:

Para fins desta Política de Segurança, os seguintes termos ficam entendidos da seguinte forma:

- **AMEAÇA:** Eventos que têm potencial lesivo, direto ou indiretamente, decorrentes de situações inesperadas e que possam comprometer os objetivos do IgesDF;
- **ATIVOS DE INFORMAÇÃO:** São meios de processamento, transmissão, processamento e armazenamento de informações e sistemas de informações, assim como locais onde se encontram esses meios e as pessoas que a eles têm acesso;

- **AUTENTICIDADE**: É a propriedade que garante a veracidade da autoria da informação, de que ela foi produzida, expedida, alterada ou descartada por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
- **CLASSIFICAÇÃO DA INFORMAÇÃO:** Consiste na identificação e definição dos níveis de proteção que o IgesDF estabelece para as informações que são processadas internamente e os seus controles de proteção necessários;
- **CONFIDENCIALIDADE**: É a propriedade que assegura que a informação será acessível somente por quem tem autorização de acesso;
- **CONFORMIDADE**: processo que visa verificar o cumprimento das normas estabelecidas.
- **CONTROLE DE ACESSO:** É um conjunto de procedimentos internos utilizados para gerenciar o acesso de pessoas autorizadas a um determinado ambiente ou informação;
- **CRIPTOGRAFIA:** É um método virtual de conversão de dados de um formato legível em um formato codificado, que tem como objetivo evitar que a informação seja compreendida ou alterada por pessoas não autorizadas;
- **DADOS PESSOAIS:** É qualquer informação que identifique direta ou indiretamente uma pessoa física em meios físicos ou digitais;
- **DISPONIBILIDADE:** É a propriedade que assegura que apenas usuários autorizados tenham acesso as informações e aos recursos associados, quando requeridos;
- **FORNECEDORES:** São todos os prestadores de serviço (pessoas físicas ou jurídicas, contratados ou subcontratados) que fornecem produtos ou serviços para a execução das atividades do IgesDf;
- **GESTÃO DE RISCOS:** É o conjunto de processos internos que permitem identificar, mapear e implementar medidas de proteção necessárias para minimizar ou eliminar os riscos internos;
- **INFORMAÇÃO:** Fica entendido como o patrimônio do Instituto de Gestão Estratégica de Saúde – IgesDF, consistente nas suas informações, que podem ser de caráter comercial, estratégico, técnico, financeiro, mercadológico, legal, de recursos humanos, ou de qualquer outra natureza, não importando se protegidas ou não de confidencialidade, desde que se encontrem armazenadas e/ou trafegadas na infraestrutura tecnológica do Instituto de Gestão Estratégica de Saúde – IgesDF;
- **INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO**: Refere-se aos componentes necessários para executar e gerenciar ambientes de TI empresariais, tais como instalações prediais, computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica;
- **INTEGRIDADE:** É a propriedade que assegura que a informação não foi alterada durante seu processo de **transporte e armazenamento;**
- **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD):** É a legislação que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado;

- **TRATAMENTO DA INFORMAÇÃO**: É toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **USO COMPARTILHADO DE DADOS:** É toda comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- **USUÁRIOS:** São todos os colaboradores com vínculo empregatício, servidores postos à disposição por órgãos ou entidades da administração centralizada ou descentralizada, federal, estadual ou municipal, não importando o regime jurídico a que estejam submetidos, prestadores de serviços que, de qualquer forma, estejam alocados na prestação de serviços, por força de contrato e colaboradores em geral.

4. DESTINATÁRIOS

Esta Política aplica-se a todos os colaboradores do Instituto de Gestão Estratégica de Saúde – IgesDF com vínculo empregatício, servidores postos à disposição pela Secretaria de Estado de Saúde, prestadores de serviços, por força de contrato e colaboradores em geral que, direta ou indiretamente, utilizem os sistemas do IgesDF para o desenvolvimento de suas atividades profissionais.

5.DIRETRIZES

Aqui no Instituto de Gestão Estratégica de Saúde – IgesDF a informação constitui-se como ativo de extrema importância, sendo fundamental para o sucesso da prestação de serviços de atenção à Saúde, merecendo, portanto, proteção e segurança adequadas.

Segurança da Informação consiste em medidas e controles aptos a proteger a confidencialidade, integridade, disponibilidade e privacidade das informações, seja em ambiente físico ou digital das diversas ameaças existentes, a fim de evitar seu uso inadequado, indevido, ilegal ou em desconformidade com nossas políticas de processos internos.

Para isto, elencamos algumas diretrizes que devem ser seguidas por todos os nossos colaboradores e fornecedores:

- As informações desenvolvidas pelos colaboradores são de propriedade exclusiva do IgesDF, assim como as informações a eles disponibilizadas, seja para execução das suas atividades diárias, seja de maneira autorizada, ou seja disponibilizadas por terceiros, devendo ser utilizadas exclusivamente para o atendimento dos objetivos internos;
- As informações devem estar devidamente protegidas e classificadas em observância as diretrizes de segurança da informação do IgesDF, em todo ciclo de vida do dado, desde a coleta, até o descarte;
- As informações internamente tratadas devem ser atribuídas a proprietários formalmente designados, sendo os mesmos responsáveis pela autorização de acesso às informações que estão sob sua responsabilidade, e em casos devidamente comprovados de tratamento indevido da informação, devendo ser apurada a responsabilidade, juntamente com o administrador que lhe concedeu o acesso;
- Os acessos às informações e aos ambientes tecnológicos do IgesDF devem ser monitorados e controlados de acordo com a classificação da informação, devendo ser revisados regularmente, de forma a serem disponibilizados apenas às pessoas autorizadas e com os privilégios necessários para o desempenho de suas atividades;
- Os equipamentos, sistemas e meios de comunicação do IgesDF estão sujeitos a monitoramento, devendo ser de conhecimento de todos os colaboradores abrangidos por esta Política;
- O IgesDF deve adotar mecanismos internos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens, e roubo e ataques cibernéticos, em todo o ciclo de vida das informações;
- As informações devem ser descartadas de forma que não seja possível sua reidentificação, seja em ambiente físico ou digital, devendo ser considerado os prazos mínimos legais ou regulatórios;
- Os contratos com empresas prestadoras de serviço que possuem acesso às informações, aos dados pessoais, aos sistemas internos ou ao ambiente do IgesDF, devem conter cláusulas ou aditivos que assegurem o cumprimento das regras internas de segurança da informação, assim como penalidades pelo seu descumprimento;
- A cultura de segurança da informação e cibernética deve ser divulgada por meio de um programa permanente de sensibilização, conscientização e capacitação;
- A gestão de continuidade de negócios deve estabelecer e manter uma estrutura estratégica e operacional apta a gerenciar a interrupção dos processos internos que suportam as atividades do IgesDF.

6.PAPÉIS E RESPONSABILIDADES:

A todos os Colaboradores abrangidos por esta Política:

- Cumprir as regras de Segurança da Informação compreendidos neste documento;

- Cumprir leis, decretos, regulamentos e normativos internos que regulem a segurança da informação e cibernética, assim como protejam os dados pessoais;
- Proteger os dados contra acessos, divulgação, modificação ou destruição não autorizados;
- Não compartilhar informações as quais tenha acesso em virtude da sua função;
- Assegurar que as informações, os sistemas e os recursos tecnológicos que sejam utilizados no dia a dia de suas atividades sejam manipulados apenas para as finalidades do IgesDF;
- Não discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos, incluindo comentários e opiniões em blogs e redes sociais;
- Comunicar imediatamente à GETIC qualquer descumprimento ou violação desta Política e/ou de suas normas e procedimentos internos.

A todos os Gestores abrangidos por esta Política:

- Orientar e assegurar a sua equipe em relação aos controles e as boas práticas de segurança da informação e proteção de dados contidos nesta Política e em normativos internos.

7.PERIODICIDADE DE REVISÃO

Esta Política de Segurança da Informação deve ser revisada no período mínimo de 1 (um) ano, ou, extraordinariamente a qualquer tempo, quando se fizer necessário.

8.REFERÊNCIAS BIBLIOGRÁFICAS:

ABNT NBR ISO 27001:2022Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2022. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.

ABNT NBR ISO 27002:2022 Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação. Rio de Janeiro, 2022. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.

9. HISTÓRICO DAS REVISÕES

Nº DA VERSÃO	DATA DA PUBLICAÇÃO	ITEM MODIFICADO
000	26/06/2023	-