POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1- ÂMBITO E VALIDADE

As diretrizes estabelecidas neste documento devem ser observadas pelo GDF Saúde e aplicam-se também a todos os ativos, equipamentos, software básico e aplicativos de propriedade do Instituto de Assistência à Saúde dos Servidores do Distrito Federal - INAS ou de entidade parceira, assim como aqueles contratados em qualquer regime.

Esta política possui validade de dois anos, a contar do dia seguinte à sua publicação, e deverá ser cumprida por todos os servidores, parceiros, consultores, especialistas ou pessoas contratadas em regime temporário, estagiários, menores aprendizes e pessoas integrantes do quadro de pessoal de empresas contratadas.

2-PRINCÍPIOS E DIRETRIZES

Os seguintes princípios norteiam a governança da segurança da informação no Instituto de Assistência à Saúde dos Servidores do Distrito Federal - INAS:

1. Adotar procedimentos padronizados e medidas para preservar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade no tratamento das informações, possuídas ou custodiadas, que possam promover impactos na continuidade das atividades da GDF Saúde;
2. Utilizar medidas de proteção das informações contra acesso, modificação, destruição ou divulgação não autorizada, garantindo sua confidencialidade, disponibilidade, integridade e não repúdio;
3. Buscar garantir a segurança dos ativos que custodiam informações do GDF Saúde e valer-se de mecanismos de controle para verificação dos fatores de risco de suas atividades, custo e valor agregado em relação à tecnologia, para garantir a segurança da informação;
4. Dispor de acordos de confidencialidade e a de não divulgação de informações confidenciais, ou sigilosas, que visam a proteção das informações do GDF Saúde, e informam os signatários das suas

responsabilidades, para proteger, usar ou divulgar a informação de maneira responsável e autorizada;

5. Valer-se de requisitos e controles de segurança quando da necessidade de acesso aos recursos de processamento da informação, ou a informação do GDF Saúde por partes externas, prestadores ou beneficiários;

6. Treinar todos os usuários quanto as instalações, sistemas, equipamentos, documentos, informações, bens e materiais do GDF Saúde, de forma a certificá-los sobre as ameaças e preocupações quanto à segurança da informação e possibilitar o uso correto desses ativos, minimizando possíveis riscos de segurança;

7. Dispor de sistema de segurança física para proteção dos acessos aos ambientes, do transporte de equipamentos e de documentação, com perímetro estabelecido de acordo com a criticidade dos locais, atividades e informações do GDF Saúde e manter em segurança e protegidos por barreiras, eletrônicas ou não, todos os recursos e instalações de processamento de informações críticas ou sensíveis às atividades do GDF Saúde, inclusive equipamentos para contingência e mídia de backup, de acordo com a avaliação dos riscos e procedimentos claramente definidos;

8. Buscar a segregação de funções e áreas para reduzir os riscos operacionais bem como as oportunidades de modificação ou uso indevido, não autorizado ou não intencional, dos ativos da organização; e também a segregação dos ambientes de recursos de desenvolvimento, teste e produção, para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais;

9. Buscar a utilização de procedimentos e diretrizes de backups que permitam, em quaisquer situações, a recuperação de softwares, sistemas, dados e documentação, armazenados em meio físico ou lógico, e que devem ser verificados e testados regularmente, para garantir sua efetividade;

10. Realizar análises críticas periódicas dos riscos de segurança e dos controles implementados bem como quando houver mudanças nos requisitos das atividades do GDF Saúde e suas prioridades, nas novas

ameaças e vulnerabilidades, visando confirmar a efetividade e adequação dos controles adotados;

11. Dispor – para os casos de terceirização do desenvolvimento de software – de acordos de licença, de evolução do Sistema e de cobrança dos requisitos contratuais com respeito à qualidade do código e à existência de garantias;

12. Implementar mecanismo que permita registrar os incidentes de segurança, tão logo sejam detectados, a fim de tratá-los adequadamente evitando sua replicação e manter um gerenciamento efetivo de incidentes para a garantia de resposta rápida, efetiva e ordenada, por meio da adoção de controles visando a manutenção das atividades do GDF Saúde;

13. Registrar, periodicamente, em relatório específico, os resultados das atividades de verificação e avaliação da governança de segurança da informação, para conhecimento e priorização do Órgão.

14. Segurança e prevenção: utilização de medidas técnicas e administrativas que garantam a proteção dos dados pessoais contra acessos não autorizados e a prevenção contra situações acidentais ou ilícitas que gerem destruição, perda, alteração, comunicação ou difusão desses dados.