DECRETO 331/2005.

São Gonçalo, 04 de novembro de 2005.

DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DE INFORMAÇÕES DA PREFEITURA DE SÃO GONÇALO.

A PREFEITURA MUNICIPAL DE SÃO GONÇALO, no uso das atribuições que lhe são conferidas pela legislação em vigor,

DECRETA:

C A P Í T U L O I

D I S P O S I Ç Õ E S I N I C I A I S

Art. 1º . A Política de Segurança de Informações aplica-se a todos os órgãos do Poder Executivo da administração direta deste município, suas autarquias e fundações, e tem por objetivos:

I. Reduzir riscos de perda de dados.

II. Minimizar possibilidade de acessos não autorizados, bem como de utilização e de alterações indevidas dos dados e sistemas de informação.

III. Garantir a confidencialidade, a integridade e a disponibilidade das informações de interesse da administração.

IV. Assegurar a continuidade das atividades desenvolvidas pelos diversos órgãos.

Artigo 2º . O Sistema Municipal de Informática abrange todos os sistemas, bases de dados e recursos de informática no âmbito da do Poder Executivo da administração direta do Município de São Gonçalo, suas autarquias e fundações.

Parágrafo 1º. A gestão do Sistema é responsabilidade do Subsecretário de Informática da Secretaria Municipal de Fazenda.

Parágrafo 2º. Cada uma das Secretarias Municipais, Autarquias e Fundações do Município designará formalmente um funcionário para exercer no âmbito daquele órgão as funções de Representante de Núcleo de Informática, com as funções definidas neste Decreto.

CAPÍTULO II

DOS PRINCÍPIOS DE SEGURANÇA

Art. 3º. Com relação ao tratamento de informações:

I. As informações são de propriedade do Município e, como tais, devem ser tomadas as medidas necessárias para protegê-las de alteração, destruição ou divulgação não autorizadas, quer sejam acidentais ou intencionais.

II. Toda informação deve ter um gestor, que será responsável pela concessão e cancelamento dos direitos de acesso.

III. O gestor também classificará as informações quanto à sua confidencialidade, integridade e disponibilidade. A Área de Informática proverá o suporte necessário aos gestores para a definição da classificação das informações.

IV. As informações devem ser identificadas de forma a serem adequadamente acessadas, manipuladas, armazenadas, transportadas e descartadas.

V. Servidores públicos e prestadores de serviço devem garantir o sigilo das informações a que tiverem acesso, tomando o cuidado necessário quanto a sua divulgação interna e externa, avaliando o seu respectivo nível estratégico.

VI. Todos os processamentos executados nos Sistemas de Informação da P.M.S.G. deverão ter suas responsabilidades conhecidas e distribuídas de forma a não serem concentrados em um mesmo grupo ou pessoas.

Art. 4º. Relativamente ao controle de acesso aos sistemas e informações:

I. Todo servidor público ou pessoa autorizada deve ter uma identificação única, pessoal e intransferível, que a torna responsável por qualquer atividade desenvolvida através dela.

II. A concessão de autorização de acesso deverá ser restrita aos recursos mínimos necessários para que os usuários desenvolvam suas atividades.

III. Sendo necessário, pode ser concedido acesso aos Prestadores de Serviço, com prazo limitado à execução de suas atividades.

Art. 5º. Constituem faltas graves:

I. O mau uso de informação pertencente ao Município e de seus recursos de informática, ou o não cumprimento de normas que visem protegê-los, constituem falta grave, e têm suas sanções previstas no Código Penal Brasileiro (Decreto Lei nº 2.848/1940), com as alterações promovidas pela Lei Federal nº 9.983, de 14.07.2000, sem prejuízo das sanções administrativas aplicáveis aos casos concretos, previstas na Lei Municipal nº 50, de 02.12.1991 (Estatuto dos Funcionários Municipais).

II. O mau uso da identificação pessoal para fins de acesso indevido a informações não autorizadas, por parte do servidor público ou qualquer outro que se relacione com a administração deste município, constitui falta prevista no Código Penal Brasileiro (Decreto Lei nº 2.848/1940), com as alterações promovidas pela Lei Federal nº 9.983, de 14/07/2000, sem prejuízo das sanções administrativas aplicáveis ao caso concreto, e previstas na Lei Municipal nº 50, de 02/12/1991 (Estatuto dos Funcionários Municipais), onde tem estabelecidas suas sanções.

Art. 6º. Quanto à capacitação dos usuários:

I. Os servidores públicos e os prestadores de serviço usuários dos sistemas deverão possuir conhecimento mínimo para a execução de suas tarefas, conhecer a Política de Segurança de Informações da Prefeitura, e serem devidamente treinados para o uso da rede e controle dos recursos de informática, antes de terem acesso a eles.

Art. 7º. Quanto à estabilidade do ambiente:

I. A disponibilização de recursos de informática somente será permitida após atendimento das recomendações desta Política, homologação pela área de Informática, e a autorização do responsável pelos respectivos recursos. Estes recursos deverão ser identificados de forma individual, inventariados, preservados, protegidos contra acessos indevidos, serem submetidos a manutenção preventiva periódica, estar com documentação atualizada e aprovada pelo Setor responsável pela Produção, e de acordo com as cláusulas contratuais pactuadas com fornecedores e com a legislação em vigor.

II. Os recursos de informática compartilhados deverão ser usados de forma a não afetar outros usuários, e desde que previamente pactuado entre os interessados.

III. Os recursos portáteis, por suas características, devem ser configurados, acondicionados e transportados atendendo às regras de segurança. O usuário do recurso portátil obriga-se à assinatura de termo de custódia, que determina os direitos e deveres quanto à utilização, posse e guarda do recurso e das informações nele armazenadas.

IV. Os sistemas devem ser testados em ambiente adequado e segregado antes de entrarem em produção.

C A P Í T U L O I I I

D A S R E S P O N S A B I L I D A D E S

Art. 8º. Caberá à Chefia de cada Setor em relação aos sistemas vinculados às suas atribuições:

I. Garantir a segurança das informações e equipamentos à sua disposição.

II. Informar ao Gestor da Informação qualquer alteração nos direitos de acesso, bem como a inclusão ou exclusão de usuários de sua área.

III. Informar ao Representante de Núcleo de Informática suas necessidades de recursos de informática.

Art. 9º. Caberá ao Representante de Núcleo de Informática, relativamente aos dados e sistemas do órgão a que está vinculado:

I. Estabelecer condições para que os sistemas e bases de dados funcionem de forma eficiente, segura e controlada.

II. Definir e homologar os treinamentos necessários para a correta e eficiente utilização dos recursos informatizados.

III. Autorizar o uso de equipamentos de informática, bem como a conexão de equipamento particular nas redes internas.

IV. Solicitar a aquisição e homologar equipamentos e aplicativos utilizados pela P.M.S.G.

V. Instalar aplicativos e sistemas adquiridos ou desenvolvidos pela P.M.S.G. e configurar as estações de trabalho, atendendo no que couber às diretrizes estabelecidas pelo Gestor do Sistema Municipal de Informática, com vistas à padronização.

VI. Autorizar a entrada e saída de recursos de sua área ou sob sua custódia, ou delegar essa autoridade a outro servidor.

VII. Garantir a integridade e disponibilidade das informações e dos recursos do ambiente informatizado disponíveis em sua área, segundo os controles estabelecidos pelo Gestor do Sistema Municipal de Informática.

VIII. Executar os procedimentos de contingência em caso de contaminação do ambiente por vírus.

IX. Efetuar cópia de segurança dos sistemas colocados em produção, bem como autorizar a restauração.

X. Avaliar as atualizações desenvolvidas pelos fornecedores de software.

Art. 10º. Caberá ao Agente de Patrimônio:

Parágrafo Único - Inventariar equipamentos de informática.

Art. 11º. Caberá ao Gestor da Informação:

I. Determinar os níveis de acesso que os usuários deverão ter às informações através de aplicativos e sistemas, solicitar formalmente estes acessos à área de informática e promover o cancelamento desses direitos.

II. Homologar, testar e autorizar a entrada em produção de sistemas e aplicativos desenvolvidos.

Art. 12º. Caberá à Diretoria de Segurança de Informações da Subsecretaria de Informática propor atualizações na Política de Segurança de Informações.

I. Definir soluções de segurança das informações para os Órgãos do Poder Executivo da Administração do Município, suas autarquias e fundações.

II. Avaliar o impacto das novas tecnologias na segurança dos dados e dos sistemas.

C A P Í T U L O I V

D A S D I S P O S I Ç Õ E S F I N A I S

Art. 13º . Cuidar da segurança e da integridade dos recursos informatizados do Município é responsabilidade de todos os usuários e funcionários em geral.

Art. 14º . É responsabilidade de todo servidor público e dos prestadores de serviço envolvidos com os sistemas de informação deste Município observar desvios dos procedimentos estabelecidos, e informá-los à sua chefia imediata.

Art. 15º . Estas diretrizes deverão ser revisadas e atualizadas pelo Gestor do Sistema Municipal de Informática sempre que necessário, ou a cada 12 (doze) meses.

Art. 16º . Constituem partes integrantes deste Decreto os Anexos I, II e III.

Art. 17º. Este Decreto entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

MARIA APARECIDA PANISSET
PREFEITA

ANEXO I

NORMAS GERAIS PARA USUÁRIOS

APRESENTAÇÃO

As presentes normas gerais para usuários integram a Política de Segurança de Informações da Prefeitura Municipal de São Gonçalo e visam a disciplinar a conduta dos servidores públicos e prestadores de serviço, em relação às bases de dados e aos recursos de informática, com vistas a garantir a segurança das informações.

1. DISPOSIÇÕES INICIAIS

1.1. Estas normas servem como base para a definição dos procedimentos que deverão ser desenvolvidos pelos responsáveis por cada processo.

1.2. As normas destinam-se a todos os usuários que tenham acesso às informações da P.M.S.G., incluindo técnicos e gestores de informações.

2. DOCUMENTOS DE REFERÊNCIA

2.1. Integram também a Política de Segurança de Informações da Prefeitura Municipal de São Gonçalo os Anexos II – Normas Gerais Técnicas, e III - Manual de Organização e Conceitos.

3. TRATAMENTO DA INFORMAÇÃO

3.1. Os recursos de informação não públicos somente deverão ser utilizados por pessoas devidamente autorizadas, sendo o seu uso limitado aos interesses da P.M.S.G. e para os fins previstos.

3.2. Todos deverão ter conhecimento dos conceitos de segurança de informações.

3.3. Deve ser mantido sigilo sobre as informações consideradas estratégicas e confidenciais, e o responsável imediato deverá ser informado sempre que informações ou aplicações críticas forem encontradas sem o devido tratamento de segurança.

3.4. As informações confidenciais ou críticas para as atividades da P.M.S.G. devem ser armazenadas de forma protegida.

3.5. Cuidar da integridade e bom funcionamento dos recursos da informação do Município é responsabilidade de todos.

3.6. É vedada a utilização de recursos de informação não autorizados ou não homologados pela área de informática, cabendo a aplicação de punição prevista no Código Penal Brasileiro

(Decreto Lei nº 2.848/40), com as alterações que lhe deu a Lei Federal nº 9.983, de 14.07.2000 e na Lei Municipal nº 50, de 02.12.1991 (Estatuto dos Funcionários Municipais).

3.7. Os sistemas e banco de dados somente poderão ser acessados a partir de estações configuradas pela área de informática responsável.

4 . S O F T W A R E

4.1. É proibida a cessão, sem autorização formal do responsável da área de informática, de cópia de software adquirido ou desenvolvido pela P.M.S.G. para benefício próprio ou de terceiros.

4.2. A utilização fora do ambiente da P.M.S.G. de cópia de software adquirido ou desenvolvido por este município somente poderá ser realizada após autorização formal do Gestor do Sistema Municipal de Informática.

5 . H A R D W A R E

5.1. A utilização de equipamentos é restrita àqueles autorizados pela área de informática.

5.2. A conexão de equipamentos particulares nas redes de dados do Município deverá ser autorizada previamente pelo responsável da área de informática.

6 . I N T E R N E T

6.1. A Internet e Intranet são consideradas aplicações críticas e devem ser garantidas as medidas de segurança para a sua utilização.

6.2. Não são permitidos os acessos a sites em desconformidade com os interesses da P.M.S.G.

6.3. A Internet só poderá ser disponibilizada através de firewall administrado pelo Órgão Gestor do Sistema Municipal de Informática.

7 . C O R R E I O E L E T R Ô N I C O

7.1. A utilização do correio eletrônico deve ser realizada em conformidade com os interesses da P.M.S.G.

7.2. O usuário deverá sempre remover as mensagens obsoletas e não mais necessárias às suas atividades.

7.3. O software utilizado deverá ser sempre o homologado pelo Gestor do Sistema Municipal de Informática.

8 . B A C K U P

8.1. O backup das informações armazenadas localmente, nas estações, será de responsabilidade do usuário. Neste caso, o usuário deverá:

- Efetuar 2 (duas) cópias de segurança;
- Manter as cópias em ambientes diferentes, seguros, indicados pelo gestor da informação;
- Realizar testes de integridade e restauração das informações copiadas; e,
- Implementar controle de acesso com senha, caso se trate de informações sensíveis.

8.2. O usuário deverá solicitar à área de informática a restauração da cópia de segurança das informações armazenadas nos servidores, que, em caso de tratar-se de informações críticas, deverá ser autorizada pelo Gestor da informação.

9 . C O N T R O L E D E A C E S S O

9.1. Os acessos do usuário às informações e aos sistemas deverão ser realizados através de **sua identificação** e senha, **únicas e não compartilhadas**. Diante da suspeita de perda de sigilo de sua senha, o usuário deverá efetuar sua troca e informar à área de informática e ao seu chefe imediato.

9.2. O tamanho mínimo da senha será de 6 (seis) caracteres alfanuméricos e, no primeiro acesso após a habilitação, o usuário terá, obrigatoriamente, que informar uma nova senha.

9.3. É proibida a adoção de senhas frágeis pelos usuários, tais como nomes próprios, palavras de vocabulário, siglas, nomes de fabricantes, datas comemorativas, dentre outras.

9.4. Considera-se fraude a tentativa, por usuários não autorizados, de quebrar a segurança do sistema ou descobrir a senha de outros usuários, e será aplicada punição prevista no Código Penal Brasileiro (Decreto Lei nº 2.848/40), com as alterações que lhe deu a Lei Federal nº 9.983, de 14.07.2000 e na Lei Municipal nº 50, de 02.12.1991 (Estatuto dos Funcionários Municipais).

9.5. Os usuários terão direito apenas aos privilégios necessários para o desempenho de suas atividades, os quais deverão ser solicitados pelos gestores da informação ou responsáveis imediatos.

9.6. Terceiros, ou prestadores de serviços, deverão ter identificação com prazo de validade temporário, de acordo com o projeto ou contrato estabelecido.

10. DESCARTE DE INFORMAÇÕES

10.1. Os arquivos e informações que não sejam mais necessários deverão ser removidos do ambiente operacional.

10.2. Quando for necessário o descarte de informações críticas ou confidenciais, ele deverá ser feito de forma irreversível, que não permita sua recuperação, respeitando-se as normas e legislação em vigor.

11. PADRONIZAÇÃO

11.1. É proibido alterar a configuração da estação de trabalho sem autorização da área de informática. Os usuários devem respeitar os padrões de hardware e software implementados.

11.2. Somente o responsável pela área de informática, ou alguém designado por ele, poderá realizar atualizações tecnológicas no ambiente informatizado.

12. COMBATE A VÍRUS

12.1. As estações de trabalho deverão, obrigatoriamente, ter o antivírus padrão instalado, configurado, ativado e atualizado.

13. ATENDIMENTO AO USUÁRIO

13.1. O usuário deverá acompanhar os técnicos de informática quando ocorrer manutenção corretiva nos equipamentos sob sua responsabilidade ou nas suas estações de trabalho.

13.2. Havendo necessidade, o técnico poderá retirar o equipamento para manutenção no laboratório, documentando a sua retirada.

13.3. A prioridade de atendimento será concedida aos equipamentos e aplicações críticas para atividades da P.M.S.G.

14. SEGURANÇA FÍSICA

14.1. A entrada e saída de pessoas não pertencentes aos ambientes críticos deverão ser registradas.

14.2. A sala de servidores, ou CPD, tem seu acesso restrito aos seus administradores ou pessoas autorizadas e acompanhadas por eles.

14.3. É proibido alimentar-se ou fumar próximo aos equipamentos de informática.

15. DISPOSIÇÕES FINAIS

15.1. Este documento terá vigência imediata após sua publicação no diário oficial.

ANEXO II

NORMAS GERAIS TÉCNICAS

APRESENTAÇÃO

As normas gerais técnicas são um conjunto de condições mínimas para atender às necessidades de segurança de informações, devendo ser cumpridas por todos os técnicos de informática e responsáveis pelos ambientes informatizados da P.M.S.G.

1. DISPOSIÇÕES INICIAIS

1.1. Estas normas servem como base para a definição de procedimentos para cada ambiente informatizado, que deverão ser desenvolvidos pelos responsáveis por cada processo e pelas áreas de informática.

2. DOCUMENTOS DE REFERÊNCIA

2.1. Anexos I – Normas Gerais para Usuários e III **-** Manual de Organização e Conceitos.

3. CONTROLE DE ACESSO

3.1. Chaves e Senhas

3.1.1. Os administradores de sistemas devem ter duas chaves distintas: uma para uso normal e outra com direitos especiais para as tarefas de administração, que somente deverá ser utilizada para este fim.

3.1.2. O acesso à informação deverá ser liberado após a autorização formal do Gestor da Informação. Haverá, no mínimo, os controles de:

- Códigos de identificação (chaves) e senha;
- Perfil de acesso; e,
- Auditoria.

3.1.3. Em todos acessos os ambientes computacionais, a configuração do tamanho mínimo da senha será de 6 (seis) caracteres alfanuméricos e, no primeiro acesso após a habilitação, o usuário terá obrigatoriamente que informar uma nova senha.

3.1.4. Os sistemas devem ser configurados visando à impossibilidade de um mesmo usuário ter mais de um acesso simultâneo, a não ser nos casos em que seja estritamente necessário.

3.1.7. As senhas serão obrigatoriamente armazenadas com criptografia.

3.1.8. Poderá ser criado um usuário sem senha, ou com senha de domínio público, exclusivamente para o compartilhamento de recursos e informações públicas, tais como impressora e área de disco de uso comum.

3.1.9. Os sistemas aplicativos, que não sejam classificados como informação pública, deverão possuir mecanismos para evitar a adoção de senhas frágeis pelos usuários, como siglas do município, nome de fabricantes, datas comemorativas, dentre outras.

3.1.10. Deverá ser permitido que o Gestor, ou pessoa por ele autorizada, reinicialize senhas para usuários que as tenham perdido.

3.1.11. Deve ser permitido aos Gestores listarem os usuários, incluindo códigos de identificação e *status* (ativo ou não), bem como informações sobre o seu perfil de acesso.

3.2. Proteção das informações

3.2.1. O cancelamento de direitos de acesso, pela área de informática, somente poderá ser efetuado mediante solicitação formal do responsável, ou por seu substituto.

3.2.2. Em situações críticas, o congelamento do acesso a um recurso poderá ser efetuado diretamente pelo seu administrador, desde que seja relatado à sua chefia imediata logo após a intervenção.

3.3. Acesso Remoto

3.3.1. Todos os equipamentos com canal de comunicação externo são considerados críticos.

3.3.2. Qualquer aplicação remota e transmissão de dados somente poderá ser disponibilizada após análise do Gestor do Sistema Municipal de Informática.

4. MANUTENÇÃO E ADMINISTRAÇÃO DO AMBIENTE

4.1. Administração

4.1.1. Deve haver substitutos capacitados para todos os administradores de sistemas dos ambientes computacionais.

4.1.2. Os sistemas operacionais deverão sofrer as atualizações desenvolvidas pelos fornecedores. A área de suporte será responsável pela implantação destas atualizações no menor prazo possível, seguindo as recomendações dos fornecedores.

4.1.3. A adoção de novas tecnologias deve ser autorizada pela Diretoria de Segurança, que elaborará, quando couber, um relatório de avaliação do impacto na segurança. Se necessário, após a implementação, a Diretoria de Segurança proporá ao Gestor do Sistema Municipal de Informática a revisão da Política de Segurança de Informações e irá requisitar ao responsável pelo recurso o desenvolvimento ou alteração nos procedimentos.

4.1.4. A administração da rede e sistemas deverá ser realizada por ferramentas previamente homologadas pelo Gestor do Sistema Municipal de Informática.

4.1.5. Os equipamentos críticos, tais como servidores e roteadores dentre outros, devem ser instalados em ambiente seguro e controlado.

4.1.6. Os acessos via Internet serão disponibilizados pelo responsável pela área de informática.

4.1.7. O administrador do correio eletrônico será o responsável pelo cadastramento e descadastramento dos usuários no correio eletrônico interno.

4.1.8. A sessão do usuário do correio eletrônico deverá ser suspensa após 5 (cinco) minutos de inatividade.

4.2. Backup

4.2.1. Toda cópia de segurança de informações sigilosas deverá ser controlada por senha, sendo o acesso físico às áreas de dados restrito e controlado.

4.2.2. A cópia de segurança dos servidores deverá ser realizada com freqüência mínima de 1 vez por (uma) semana.

4.2.3. As mídias de cópias de segurança devem ser descartadas, de forma a obedecer à classificação das informações nelas contidas, e de acordo com os parâmetros especificados pelo seu fabricante.

4.2.4. O teste de restauração e integridade das cópias de segurança ter periodicidade máxima de 180 (cento e oitenta) dias.

4.3. Auditoria

4.3.1. Todos os acessos aos aplicativos deverão ser registrados em auditoria, documentando-se a hora de início e fim da transação, o código de identificação do usuário, a data e o tipo de alteração realizada. Os sistemas operacionais deverão fazer os mesmos registros, quando possível.

4.3.2. Os registros de ambientes críticos deverão ser auditadas com periodicidade definida pela Auditoria de Sistemas.

4.4. Combate a vírus

4.4.1. Os casos de contaminação por vírus deverão ser comunicados imediatamente ao help-desk.

4.5. Recursos

4.5.1. Toda instalação de recursos deverá seguir controle de segurança física.

4.5.2. Recursos somente deverão ser disponibilizados à produção após testes em ambiente segregado e controlado. Os recursos têm que estar devidamente documentados e com esta documentação aprovada pelo setor responsável pela produção.

4.5.3. Os responsáveis da área de informática deverão homologar todos os recursos informatizados utilizados pela P.M.S.G. Nos casos de software aplicativo, a autorização final será dada pelo gestor da informação, ouvido o Gestor do Sistema Municipal de Informática, quanto às questões técnicas envolvidas.

4.5.4. Todo software sensível e aplicações críticas devem ser instalados ou disponibilizados de modo que o usuário não possa alterar as suas configurações.

4.5.5. Os testes devem ser efetuados usando dados fictícios. Testes paralelos, com dados de produção, ou de aceitação devem ser considerados trabalho de produção, e, portanto, devem ser efetuados pelo setor responsável pela produção.

4.5.6. Somente o setor responsável pela produção pode acessar dados de produção, salvo com autorização do gestor da informação.

4.5.7. Deverão ser criadas rotinas de manutenção preventiva nos equipamentos.

4.5.8. Deve ser mantida atualizada a relação dos programas, sistemas e equipamentos utilizados no ambiente sob responsabilidade da área de informática.

4.5.9. Os diretórios das aplicações de produção deverão ter controle de acesso mantido pelo setor responsável pela produção e descritos na documentação do sistema.

4.5.10. Todas as aplicações críticas devem ser controladas por senhas de acesso.

4.5.11. Deve-se evitar a extração de dados de um sistema para alimentar outro. Esta ação só será permitida após análise e aprovação das áreas de administração de Dados e Produção do Gestor do Sistema Municipal de Informática.

4.6. Plano de Contingência

4.6.1. Deverá ser elaborado plano de contingência para os recursos informatizados considerados críticos, de forma a garantir a continuidade das atividades da P.M.S.G. em casos de sinistro ou acidente.

4.6.2. Deverá haver rotina de teste e reavaliação do plano de contingência com periodicidade máxima de 1 (um) ano.

4.7. Desenvolvimento e documentação de sistemas

4.7.1. Os sistemas aplicativos devem ser baseados na metodologia de desenvolvimento definida pelo Gestor do Sistema Municipal de Informática e de modelagem de dados definidos pela Administração de Dados.

4.7.2. Os sistemas aplicativos desenvolvidos para a P.M.S.G. são de sua propriedade e só poderão ser cedidos a terceiros com prévia autorização do gestor e do Gestor do Sistema Municipal de Informática.

4.7.3. A documentação dos sistemas e aplicativos desenvolvidos deverá ser elaborada por quem o desenvolveu observando-se as normas estabelecidas pelo Gestor do Sistema Municipal de Informática.

4.7.4. Cada sistema deve processar seus próprios dados. Deve ser privilegiada a integração e não a criação de interfaces entre Sistemas, com o apoio das áreas de Administração de Dados do Gestor do Sistema Municipal de Informática.

5. DISPOSIÇÕES FINAIS

5.1. Cabe à Diretoria de Segurança de Informações rever permanentemente este documento**,** e ao Órgão Gestor do Sistema Municipal de Informática aprová-lo.

5.2. Este documento terá vigência imediata após sua publicação no diário oficial.

5.3. O prazo máximo para revisão deste documento é de 1 (um) ano, a contar da sua publicação.

ANEXO III

MANUAL DE ORGANIZAÇÕES E CONCEITOS

O B J E T I V O

Este manual descreve e define os termos e expressões constantes nos documentos que integram a Política de Segurança de Informações da P.M.S.G.

D E F I N I Ç Õ E S

Acesso Físico: Trânsito (entrada ou saída) de pessoas em um ambiente, seja uma sala, um cofre ou uma área.

Acesso Lógico: Procedimento através do qual é permitido a um usuário do ambiente de informática, os acessos às informações armazenadas em meio magnético. Somente deverá ser liberado quando atender a todos os mecanismos de proteção disponíveis na instalação.

Acesso Remoto: A capacidade de se conectar a uma rede utilizando recursos instalados em local diverso. Geralmente, isso implica uso de um computador, um modem e um programa de acesso remoto para estabelecer conexão ao servidor de rede.

Administração de Dados: Responsável por garantir a integridade dos dados e **os** acessos às diversas bases, através da e implantação de um Modelo Global de Dados.

Administrador de Rede (ou Sistemas): Responsável por gerenciar, monitorar e configurar a rede, ou o sistema, e mantê-los funcionando de forma satisfatória.

Administrador do Recurso: Responsável por determinado recurso, seja ele hardware ou software, com função de controle e gerência.

Ambiente Computacional: Ambiente lógico composto de software e controlado por sistemas operacionais.

Ambiente Informatizado: Ambiente físico onde se localizam estações de trabalho, servidores de rede e equipamentos de apoio que provêem o processamento e o armazenamento das informações.

Ambiente Operacional: Ambiente onde são executados os aplicativos e sistemas da P.M.S.G.

Ambiente Segregado e Controlado: Local com funções definidas e separado de outros com funções diversas. O controle se dá através de procedimentos que registram as entradas e saídas das informações do ambiente, e essas transações só ocorrem com as devidas autorizações.

Antivírus: *Software* que identifica e remove vírus de computador.

Aplicação Crítica: Normalmente uma aplicação que atualiza valores ou controla autorizações de acesso e/ou trata de informações classificadas como sigilosas ou vitais para a execução das atividades-fim do usuário.

Aplicativo (ou **Aplicação**)**:** Programa ou grupo de programas adquiridos ou desenvolvidos para determinado fim, tais como processador de textos, sistema de banco de dados, planilha eletrônica e sistemas específicos.

Área de Informática: Área responsável pelo processamento e armazenamento da informação. Viabiliza as especificações formuladas pelo Gestor da Informação em conformidade com os procedimentos estabelecidos pelo Gestor do Sistema Municipal de Informática.

Área de Segurança: Área responsável pela operacionalização dos conceitos de segurança.

Área de Suporte: Grupo de pessoas responsável pela instalação e configuração de *hardware* e *software,* e apoio aos usuários da P.M.S.G.

Arquivo de Log (ou simplesmente **Log**)**:** Arquivo em que são gravados registros relativos a transações executadas em um serviço informatizado.

Backup (ou Cópia de Segurança): Um substituto ou alternativa para um recurso. O termo *backup* refere-se, usualmente, a um disco ou fita que contém uma cópia de informações.

Base de Dados: São informações organizadas, interrelacionadas e armazenadas em meio magnético.

Diretoria de Segurança de Informações: Grupo de pessoas formado por representantes das áreas de tecnologia e de gestores, com o objetivo de propor soluções de segurança de informação ao Gestor do Sistema Municipal de Informática.

Chave de Acesso: Identificação do usuário (*user-id*) do ambiente computacional.

Classificação da Informação: É o grau de confidencialidade de uma informação (confidencial, restrita, pública) e a que tipo de tratamento ela está sujeita (identificação, acesso, distribuição, uso em correios e fax, reprodução, estocagem, descarte e transporte).

Correio Eletrônico (ou e-mail): Serviço de comunicação que consiste no envio e armazenamento de mensagens através de redes de computadores.

Criptografia: Técnica utilizada para converter informações num código secreto, com objetivo de segurança, para que não possam ser utilizadas ou lidas até serem decodificadas.

Equipamento Crítico: Dispositivo que armazena informações classificadas como críticas ou que possui sistema de emulação ou ainda que executa aplicações críticas.

Estação de Trabalho: Refere-se a qualquer computador conectado a uma rede.

Ferramenta de Segurança: Dispositivo de *hardware* ou *software* destinado a proteger e controlar os acessos ao conjunto de informações da empresa, de acordo com a política de segurança estabelecida.

Firewall: Dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes.

Gestores da Informação: Usuário proprietário da informação, responsável por sua criação e classificação, pelos recursos sob sua responsabilidade, acesso aos locais restritos da sua Unidade, bem como por definir os direitos de cada usuário.

Hardware: Equipamentos físicos ou dispositivos mecânicos, elétricos ou eletrônicos, que compõem os equipamentos computacionais.

Homologação: Análise da funcionalidade, testes e aprovações necessárias para a implantação de recursos informatizados.

Informação Confidencial: É toda informação cujo conhecimento deva ficar restrito a uma quantidade reduzida de pessoas autorizadas. Este tipo de informação requer alto grau de controle e proteção contra acessos não-autorizados.

Informação Crítica: É toda informação considerada vital para a continuidade dos processos e operações da P.M.S.G., cuja perda ou indisponibilidade por um determinado período de tempo possa provocar prejuízos irreparáveis.

Informação Pública: É toda informação cujo conhecimento não necessita ficar restrito a um determinado grupo de pessoas, podendo ser liberado para qualquer cidadão que o solicite, sejam eles servidores públicos municipais, prestadores de serviço ou não.

Informação Restrita: É toda informação cujo acesso deva ser limitado a um certo grupo de pessoas, em função de alguma legislação ou norma específica.

Integridade: Capacidade efetiva de a informação estar intacta e garantida contra perda, dano ou modificação não autorizada (indevida), realizada maliciosa ou acidentalmente.

Internet: Rede de computadores de alcance mundial conectados entre si. Considerada a "rede das redes", originalmente criada nos EUA, se tornou uma associação mundial de redes interligadas.

Login (ou **log on**)**:** Procedimento para que um sistema de computador ou uma rede reconheça o usuário **e** seus direitos de acesso**,** de tal forma que ele possa iniciar uma sessão de trabalho.

Manutenção Preventiva: Conjunto de operações para revisão, inspeção e limpeza dos recursos informatizados, objetivando corrigir, reparar pequenas falhas e manter a sua conservação**,** minimizando a ocorrência de problemas.

Mídia: Dispositivos nos quais as informações podem ser armazenadas, incluindo, entre outros, *hard disks* (ou discos rígidos), *floppy disks* (ou *disquetes*), CD-ROMs e fitas magnéticas. Em redes de computadores, mídia refere-se também aos cabos (ex.: cabo coaxial, fibra ótica) que interligam estações de trabalho.

Patch: Uma correção para um erro de programa. O patch deve ser submetido a partir de instruções do próprio fabricante do *software*.

Recursos de Informática: São os recursos que transformam, transportam, guardam e descartam informações, além dos próprios dados e informações. Podem ser equipamentos computacionais, conexões para redes de computadores, serviços de Internet, banco de dados, sistemas operacionais, sistemas e aplicativos que manipulam direta ou indiretamente informações.

Rede: Um grupo de dois ou mais sistemas de computador interligados. Quanto à disposição dos computadores, as redes podem ser classificadas como: local area network (LAN) – os computadores estão geograficamente próximos (geralmente, no mesmo prédio); wide-area network (WAN) – os computadores estão mais distantes, uns dos outros, e são conectados através de linhas telefônicas, ondas de rádio ou via satélite.

Senha: Uma série secreta de caracteres que habilita um usuário para acesso a um arquivo, computador ou programa. A senha autentica a identidade de uma chave de acesso.

Setor de Produção: Responsável pela execução de rotinas que não possam ou não devam ser executados pelos usuários finais dos sistemas ou outros setores da área de informática.

Sistema: Um conjunto de várias funções interligadas que automatizam um processo.

Software: Conjunto de programas, procedimentos, regras e documentação referentes à operação de um sistema, armazenado eletronicamente. Ex. sistemas aplicativos, montadores, compiladores, sub-rotinas.

Software Homologado: *Software* certificado tecnicamente pela Área de Informática em relação à aderência e compatibilidade com o ambiente informatizado da P.M.S.G.

Software Licenciado: Refere-se, genericamente, a programas, dados e documentação de propriedade de terceiros, cujo uso tenha sido licenciado para a P.M.S.G. e tenha seus direitos autorais protegidos (*copyright*).

Software Sensível: Sistemas essenciais ao desenvolvimento das atividades da P.M.S.G, e aplicativos de segurança e de disponibilizarão de informações através de redes, tais como antivírus, software de comunicação e emulador de terminal.

Usuário: Qualquer pessoa que foi autorizada pelo Gestor, a ler, inserir ou atualizar informações.

Vírus: Um programa ou pedaço de código que é introduzido em um computador sem conhecimento do usuário e, quando executado, corrompe a operação normal do sistema. Todos os vírus são fabricados. Um vírus simples que possa copiar a si próprio continuamente é relativamente fácil de produzir. Mesmo um vírus simples é perigoso porque ele pode rapidamente utilizar toda a memória disponível e levar o sistema a uma interrupção. O tipo mais perigoso de vírus é aquele capaz de reproduzir-se através da rede e burlar sistemas de segurança.