

XII - vedação do uso de credenciais de terceiros (que não sejam membros, servidores e colaboradores) para acessar sistemas, internet, intranet, correio eletrônico e rede do Ministério Público, com vista ao desempenho de qualquer tipo de atividade;

XIII - uso e aplicação da prática de mesa limpa e tela de computador protegida;

XIV - adoção da prática de exclusão das lixeiras de informações críticas e sensíveis;

XV - utilização de sistemas e aplicativos após treinamento operacional específico, seguindo definições e procedimentos registrados em manuais ou documentos similares;

XVI - acompanhamento de toda e qualquer manutenção preventiva e corretiva realizada em equipamentos sob sua responsabilidade;

XVII - obrigatoriedade da ciência e do conhecimento de todo material referente à segurança da informação, disponibilizado pelo Ministério Público;

XVIII - tratamento de documentos adequado e compatível com seu grau de sigilo;

XIX - capacitação e desenvolvimento da equipe de tecnologia da informação do Ministério Público em segurança da informação;

XX - conscientização dos membros, servidores e colaboradores do Ministério Público quanto às ameaças externas (vírus, interceptação de mensagens e dados, grampos e fraudes e tentativas que ensejam o roubo de senhas) que possam afetar ou ameaçar a segurança das informações da Instituição;

XXI - adoção da prática de não abordagem e não discussão, em ambientes públicos e áreas expostas, de assuntos relacionados ao trabalho;

XXII - esclarecimento imediato das dúvidas relacionadas à Política, às Normas e aos Procedimentos de Segurança da Informação, com o devido conhecimento e registro; e

XXIII - vedação a membro, servidor ou colaborador do Ministério Público de:

a) conectar, na rede institucional do Ministério Público, equipamentos não autorizados;

b) alterar nomes padronizados dos ativos;

c) compartilhar com terceiros conta do correio eletrônico institucional;

d) acessar e divulgar informações que contenham material obscuro, apologia ao fanatismo, práticas religiosas, político-partidárias e qualquer forma de discriminação ou material que, explícita ou implicitamente, se refira à conduta imoral;

e) fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte;

f) alimentar-se próximo aos servidores de rede e estações de trabalho; e

g) fazer cópia não autorizada de softwares adquiridos ou desenvolvidos pelo Ministério Público.

Art. 6º São diretrizes relativas à operação e comunicação:

I - responsabilização pela criação, atualização, análise crítica e registro de normas, procedimentos, documentação de sistemas, recursos tecnológicos, ambiente de rede e configurações de recursos de tecnologia da informação;

II - armazenamento e disponibilização de toda e qualquer documentação institucional em local seguro, com acesso controlado e monitorado;

III - armazenamento e proteção adequada de documentos e arquivos contendo informações confidenciais;

IV - garantia da tramitação segura de documentos no âmbito do Ministério Público;

V - manutenção sistemática da documentação institucional atualizada;

VI - exigência e obrigatoriedade da prévia análise de impacto, priorização, aprovação e plano de retrocesso para as mudanças em ativos informacionais do Ministério Público;

VII - uso de aplicações de comunicação remotas e transmissões de dados com recursos de tecnologia da informação homologados e precedidos de aprovação formal do Ministério Público;

VIII - armazenamento de informações críticas e estratégicas nos servidores da rede corporativa e em áreas protegidas;

IX - transporte de equipamentos e notebooks exclusivamente por meio de malas apropriadas;

X - remoção de toda informação classificada como confidencial e restrita, antes de qualquer manutenção, alienação ou reutilização de equipamentos;

XI - uso único e exclusivo dos serviços de help desk do Ministério Público como suporte para solução de problemas tecnológicos ou do ambiente de tecnologia da informação;

XII - proibição de acesso à informação institucional que não seja explicitamente autorizado;

XIII - vedação do transporte de informações confidenciais do Ministério Público sem a devida autorização e proteção e em qualquer meio, como CD, DVD, disquete, pen-drive, papel etc.; e

XIV - proibição de abrir ou executar arquivos de origem desconhecida.

Art. 7º São diretrizes relativas ao ambiente de redes:

I - normatização e regulamentação de procedimentos para a utilização correta do ambiente de rede;

II - garantia da continuidade do fornecimento de energia elétrica, em caso de interrupção, durante o tempo necessário à preservação dos equipamentos centrais de rede e dos demais que sejam essenciais;

III - garantia de estruturas de contingência para atendimento a situações emergenciais;

IV - disponibilização de recursos e estruturas tecnológicos adequados aos padrões de segurança do Ministério Público;

V - adoção de manutenções preventivas periódicas e sistemáticas nos equipamentos instalados;

VI - liberação dos ativos de tecnologia de informação para uso condicionada à efetiva homologação e documentação;

VII - exigência de autorização formal para a realização de intervenções e manutenções no ambiente de rede ou estações de trabalho;

VIII - supervisão das intervenções e manutenções realizadas no ambiente de rede;

IX - controle sistemático da utilização de equipamentos de terceiros na rede de informática do Ministério Público;

X - proteção contra ameaças externas e internas à rede e às de informações que nela trafegam;

XI - monitoramento e documentação do ambiente de rede, assegurando a confidencialidade, a integridade e a disponibilidade das informações que trafegam nesse ambiente;

XII - utilização de mecanismos de segurança nas transações de rede;

XIII - manutenção de equipamentos sobressalentes de tecnologia da informação para situações emergenciais; e

XIV - estruturação da rede do Ministério Público, visando integrar os serviços de voz e dados, facilitar o gerenciamento e o controle da rede física e evitar eventuais violações.

Art. 8º São diretrizes relativas à internet e intranet:

I - normatização e regulamentação de procedimentos para a utilização da internet e intranet, com a exigência de seu cumprimento;

II - adoção de ferramentas e procedimentos de segurança para os ambientes de internet e intranet;

III - restrição e controle das vulnerabilidades nos ambientes de internet e intranet; e

IV - ativação e monitoramento de logs (relatórios de ocorrências) de segurança;

Art. 9º São diretrizes relativas a firewall e antivírus:

I - procedimento formal de atualização do software de firewall e antivírus em todos os ativos de informática instalados no Ministério Público, conforme instruções e determinações do fabricante; e

II - manutenção sempre ativa do firewall e de programas antivírus.

Art. 10 São diretrizes relativas ao correio eletrônico:

I - normatização e regulamentação de procedimentos para o uso do correio eletrônico;

II - estabelecimento de limite máximo para o tamanho de caixa de entrada e anexos;

III - adoção de procedimentos padrão para garantir a segurança das informações veiculadas pelo correio eletrônico;

IV - garantia, junto ao provedor de serviços de e-mail, de bloqueio de relay, de modo a evitar o envio de mensagens com falsos remetentes, a partir de endereços externos ao Ministério Público;

V - utilização de sistema ou soluções de criptografia para envio e recebimento de mensagens contendo informações sigilosas ou sensíveis, por meio do correio eletrônico;

VI - encaminhamento imediato, ao DINF, dos alertas de vírus recebidos pelo correio eletrônico;

VII - utilização do correio eletrônico em obediência aos padrões estabelecidos pelo Ministério Público; e

VIII - adoção da prática de submissão ao programa antivírus dos anexos recebidos pelo correio eletrônico.

Art. 11 São diretrizes relativas ao desenvolvimento e manutenção de sistemas de informação:

I - definição dos requisitos de controle de segurança para novos sistemas ou melhorias em sistemas existentes;

II - normatização e padronização do requerimento de novos e a solicitação de manutenção de sistemas de informação pertencentes ao Ministério Público do Estado do Pará;

III - estabelecimento de mecanismos de proteção de direitos autorais para sistemas e aplicativos desenvolvidos internamente ou por terceiros;

IV - definição formal das responsabilidades pelos sistemas e aplicativos, por área funcional e técnica;

V - definição de procedimentos de validação dos dados de entrada, visando à garantia de sua correção, adequação e apropriação;

VI - definição de procedimentos para validação dos dados de saída das aplicações, visando assegurar a correção, a adequação e a apropriação do processamento das informações armazenadas às circunstâncias;

VII - definição de procedimentos de controles criptográficos, visando à proteção das informações;

VIII - impedimento do uso de bancos de dados operacionais (de produção) que contenham informações de natureza pessoal ou consideradas sensíveis como fonte de dados de teste;

IX - aplicação do processo de gestão de mudanças nas alterações e mudanças nos sistemas de informações da Instituição;

X - desenvolvimento, implantação e manutenção de sistemas e aplicativos mediante adoção de metodologias e padrões de plataforma e de instalação, além de ferramentas que priorizam a segurança da informação;

XI - adoção de procedimentos de contingenciamento para sistemas e aplicativos críticos, visando garantir a continuidade da ação institucional;

XII - monitoramento de todos os arquivos de logs (ocorrências) previamente configurados, visando à identificação de falhas, às violações de segurança e à recuperação de dados;

XIII - manutenção de ambientes específicos, que reflitam o ambiente de produção, para desenvolvimento e homologação de sistemas;

XIV - armazenamento, em ambiente seguro, das versões fonte e executável de sistemas e aplicativos em desenvolvimento;

XV - adoção de padrões de procedimentos seguros para a importação e exportação de dados;

XVI - adoção de procedimentos uniformes e padronizados para desativar sistemas e aplicativos não mais utilizados;

XVII - definição de procedimentos para supervisão e monitoramento do desenvolvimento de sistemas por empresas terceirizadas;

XVIII - vedação de manutenção e utilização de sistemas de informação não desenvolvidos ou autorizados pelo DINF;

XIX - restrição de acesso ao banco de dados de produção mediante sistemas, priorizando o uso de ferramentas alternativas; e

XX - realização de auditorias nos sistemas de informação do Ministério Público, visando ao atendimento às conformidades legais e à minimização de riscos de interrupções nas ações institucionais.

Art. 12 São diretrizes relativas ao controle de acesso:

I - normatização e regulamentação de procedimentos de controle de acesso ao ambiente de rede, à internet e intranet, aos serviços, aplicativos e sistemas de informações, inclusive à informação e sistemas sensíveis (críticos e que contêm informações sigilosas);

II - controle, de forma centralizada, do acesso ao ambiente e aos serviços de rede, aos aplicativos e sistemas de informação, com a utilização de procedimentos formais compatíveis com o perfil do usuário e com os níveis de autorização;

III - controle do acesso a códigos-fonte de programa e de itens associados (projetos e especificações), prevenindo a introdução de funcionalidade não autorizada e evitando mudanças não intencionais;

IV - definição e implantação de procedimentos formais de controle para criação, alteração, bloqueio, exclusão, reutilização e expiração automática de senhas de acesso ao ambiente e aos serviços de rede, aos aplicativos e sistemas de informação, ao correio eletrônico, à transferência de arquivos, aos servidores e outros;

V - implantação de padrões seguros para nomenclatura de senhas e de usuários;

VI - definição e implantação de mecanismos de gerenciamento de privilégios;

VII - controle de acesso à intranet e internet de acordo com os objetivos institucionais;

VIII - normatização e regulamentação de procedimentos e configurações seguras para os bancos de dados dos sistemas em produção, visando ao bloqueio de acessos indevidos;

IX - bloqueio ou desabilitação de usuários coletivos ou não autorizados a acessar o ambiente e os serviços de rede, os aplicativos, sistemas de informação, servidores e outros, e a avaliação das eventuais exceções a cargo de cada unidade responsável; e

X - manutenção de procedimentos para desabilitação de acessos ao ambiente e aos serviços de rede, aos aplicativos, sistemas de informação, servidores e outros, pelo tempo de sua inatividade.

Art. 13 São diretrizes relativas ao armazenamento e backup:

I - adoção de procedimentos formais de backup (cópia de segurança) e restore (recuperação) para todo o acervo de software e dados sob a responsabilidade do Ministério Público, de acordo com o perfil e especificidades de utilização;

II - monitoramento e inspeção sistemática dos registros de ocorrências das rotinas de backup;

III - adoção de procedimentos para efetuar testes de recuperação, de acordo com o perfil e a especificidade da cópia de segurança;

IV - disponibilização de local adequado e seguro para o armazenamento de mídias originais de softwares e aplicativos adquiridos, juntamente com as versões definitivas (aprovadas)