SECRETARIA ESPECIAL DE ESTADO DE INFRAESTRUTURA E LOGÍSTICA PARA O DESENVOLVIMENTO SUSTENTÁVEL

Instituto de Desenvolvimento Florestal do Estado do Pará

CAPÍTULO II
NORMAS TÉCNICAS

A**rt. 13.** Este capítulo determina um conjunto de regras a serem seguidas pela área de informática do Instituto de Desenvolvimento Florestal do Estado do Pará a fim de promover a segurança das informações e dos recursos tecnológicos.

DA ADMINISTRAÇÃO DOS RECURSOS TECNOLÓGICOS

Art. 14. A administração dos recursos tecnológicos deve ser realizada por ferramentas previamente homologadas e por pessoal capacitado.

§ 1°. Deve haver substitutos para todos os gestores de recursos tecnológicos e para quem execute processos críticos, assim indicados pela Coordenadoria de Informática.

§ 2°. Os sistemas operacionais e demais ferramentas devem possuir contrato de suporte técnico e devem sofrer as atualizações desenvolvidas pelos fornecedores, ficando a área de suporte responsável pela implantação destas atualizações e seguindo as recomendações dos fabricantes.

§ 3°. Deve ser exigido dos colaboradores e prestadores de serviço o atendimento às normas contidas neste documento, comprovado por meio documental.

§ 4°. Deve ser monitorada permanentemente a ocorrência de violações de segurança que possam causar prejuízos, com entrega de indicadores

§ 5°. A Informática definirá especificamente as ocorrências a serem monitoradas em cumprimento ao parágrafo anterior.

§ 6°. É necessário manter registro de ocorrência de eventos relevantes para efeito de histórico.

§ 7°. A adoção de novas tecnologias deve ser do conhecimento prévio da Informática.

DO CONTROLE DE ACESSO

Art. 15. O controle de acesso aos sistemas e recursos tecnológicos deve ser feito por meio de código de acesso ou qualquer outro tipo de identificação, sempre pessoal e intransferível, definido pelo seu respectivo gestor.

§ 1°. No caso de código de acesso, este deve preferencialmente ser a matrícula do servidor, e sua senha deve ser armazenada com criptografia homologada pela Informática.

§ 2°. Na concessão de senha, esta será informada ao usuário, que deverá proceder a troca no primeiro acesso.

§ 3°. É permitido apenas ao gestor do recurso, ou pessoa por ele autorizada, reinicializar senhas para usuários que as tenham perdido, desde que o pedido seja requerido formalmente para registro e atendidos os requisitos de confirmação do usuário.

§ 4°. Deve existir mecanismos que dificultem a quebra de senha através de:

I – Bloqueio após um número pré determinado de tentativas erradas;

II – Imposição de troca de senha ao usuário dentro de um intervalo de tempo;

III – Verificação de fragilidade de senha.

§ 5°. Possuir a senha de administrador de qualquer recurso não dá o direito de utilizá-la injustificadamente.

Art. 16. O servidor lotado neste Instituto deverá ter acesso apenas aos recursos e sistemas necessários ao desempenho de suas funções.

§ 1°. A concessão de acesso deve ser feita através de perfis de acesso.

§ 2°. O perfil do usuário deve refletir as atribuições funcionais do servidor, tendo como base seu cargo, lotação e/ou nível hierárquico.

§ 3°. O perfil de acesso deve ser revogado quando o servidor:

I - Encontrar-se afastado de suas funções por qualquer motivo;

II - Não mais preencher os requisitos necessários para possuí-lo em função de remoção ou exoneração;

III – For desligado deste Instituto.

§ 4°. Os casos omissos serão tratados pela Informática em conjunto com a unidade administrativa à qual o servidor está subordinado e quando não resolvidos, pela Direção Geral.

DO DESENVOLVIMENTO DE SOFTWARE

Art. 17. Os sistemas e aplicativos devem ser baseados na metodologia de desenvolvimento adotada pela área de informática.

§ 1°. O ambiente de desenvolvimento deve possuir mecanismos que garantam a confiabilidade dos códigos fonte e executáveis em produção, utilizando ferramenta de gerenciamento de versões com procedimentos de cópia de segurança, cabendo ao administrador do sistema a responsabilidade pela transferência de objetos para o ambiente de produção.

§ 2°. A realização de testes somente deve ser feita na base de dados de desenvolvimento.

§ 3°. Deve haver registros de alterações nos dados referentes a receitas e despesas, cadastro de contribuintes, e de tudo que for relevante para proteger os sistemas de fraudes contra o Instituto.

§ 4°. A documentação dos sistemas e aplicativos desenvolvidos deve ser elaborada com a participação de usuários, observando as normas estabelecidas pelo setor de informática.

§ 5°. Deve haver suporte técnico capacitado para dar manutenção em qualquer código fonte em produção.

§ 6°. Alterações em código fonte devem ser precedidas de abertura de chamado, descrevendo as modificações e seu solicitante.

§ 7°. Toda alteração deve atender aos requisitos satisfatórios de acabamento e controle de qualidade.

§ 8°. Os sistemas adquiridos de terceiros ou desenvolvidos internamente são de propriedade deste Instituto e só podem ser cedidos a terceiros com previa autorização do setor de informática, observadas as normas contratuais.

DO AMBIENTE DE REDE

Art. 18. O ambiente de rede deve compartilhar recursos e informações de forma segura, de modo a garantir a sua disponibilidade, confidencialidade e integridade.

§ 1°. Os recursos disponibilizados pela rede devem possuir mecanismos corporativos de proteção dos dados que trafegam internamente, bem como proteção contra ameaças externas, devendo estes estarem sempre atualizados.

§ 2°. O setor de informática deverá gerenciar o espaço de memória disponível nos servidores da rede para cada usuário/ unidade de trabalho e manter os mesmos informados sobre o limite de armazenamento de informações.

Art. 19. Todos os equipamentos com canal de comunicação externo são considerados críticos.

§ 1°. O acesso externo deve ser controlado e registrado, passando obrigatoriamente por um ponto de controle com características e formas de operação definidas pela área de informática.

§ 2°. Qualquer aplicação remota e transmissão de dados somente podem ser disponibilizadas após análise da Informática.

DO BANCO DE DADOS

Art. 20. Todos os bancos de dados dos sistemas corporativos deste Instituto são considerados recursos críticos, devendo ser garantida a integridade, confidencialidade e disponibilidade dos dados.

§ 1°. Deve haver procedimento de controle e registro de acessos e de transações realizadas no banco de dados de produção.

§ 2°. Deve haver uma Política de Cópias de Segurança devidamente documentada e homologada pelo Setor da Informática.

§ 3°. Operações que impliquem em re-processamento ou atualização de um grande volume de dados devem ser registradas, bem como mudança de estrutura, retorno de backup e paradas de funcionamento do banco de dados.

DAS CÓPIAS DE SEGURANÇA E DESCARTE

Art. 21. A geração de cópias de segurança deve ocorrer de acordo com a Política de Cópias de Segurança adotada pela área de informática.

§ 1°. É necessário que se preserve a compatibilidade com o ambiente operacional e físico da época da geração da cópia de segurança.

§ 2°. As cópias de segurança devem ser guardadas em local com controle de acesso físico e fora do prédio no qual foram geradas, ou onde se encontra a fonte principal da informação.

§ 3°. Deve existir teste de restauração de backup devidamente documentado, com periodicidade máxima definida no plano de contingência correspondente.

DOS RECURSOS TECNOLÓGICOS

Art. 22. Toda entrada e saída de equipamentos de informática nos prédios deste Instituto devem ser registradas e autorizadas pelo setor de informática local.

§ 1°. Esse registro não exclui outros necessários ao controle de patrimônio.

§ 2°. Cabe ao setor de informática local a movimentação interna de equipamentos bem como sua instalação e configuração, devidamente documentadas.

§ 3°. O setor de informática local deve avaliar possíveis riscos à integridade dos equipamentos tais como calor, chuva, poluição, radiação, entre outros, procedendo a devida adequação ou, se for necessário, remeter o fato à administração de informática central.

Art. 23. Os equipamentos críticos, tais como servidores e roteadores, dentre outros, devem ser instalados em ambiente seguro e controlado, com garantia de continuidade de energia elétrica.

§ 1°. O acesso a esse ambiente deve ser restrito apenas aos técnicos e administradores responsáveis pelos equipamentos.

§ 2°. Deve haver controles que garantam temperatura adequada, além de outros que visem proteger o equipamento contra quaisquer ameaças.

§ 3°. Deve haver reserva técnica para os equipamentos críticos.

DO PLANO DE CONTINGÊNCIA

Art. 24. Deve haver Planos de Contingência para os recursos informatizados considerados críticos.

§ 1°. Os planos de contingência devem abranger a recuperação imediata de serviços essenciais bem como restabelecer a continuidade das atividades deste Instituto em caso de sinistro, acidente ou qualquer outro tipo de interrupção.

§ 2°. Cabe aos responsáveis pelos processos críticos elaborar os planos e coordenar a sua execução.

§ 3°. Devem ser implementadas rotinas de teste dos planos de contingência com o objetivo de avaliar sua eficácia.

§ 4°. Cada plano de contingência deve estar difundido entre os responsáveis por sua execução e suas chefias.

§ 5°. O conjunto dos Planos de Contingência dos recursos críticos compõe o Plano de Continuidade de Negócio, que será homologado pelo Núcleo da Informação(informática).

§ 6°. Um exemplar desse documento deve ser guardado em local seguro, preferencialmente junto com as cópias de segurança.

DOS PROCEDIMENTOS DE AUDITORIA

Art. 25. A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas e padrões.

§ 1°. Cabe a Informática realizar auditoria nos sistemas e procedimentos executados pelo próprio Setor.

§ 2°. Deve constar dos procedimentos de auditoria a sua periodicidade, forma de verificação e sua duração.

§ 3°. O resultado da auditoria deve ser formalizado em um relatório que apontará as não conformidades encontradas, bem como as medidas de correção e melhoria a serem encaminhadas e adotadas pelas gerências.

DAS DISPOSIÇÕES FINAIS

Art. 26. Ao setor de informática do IDEFLOR cabe o monitoramento e gerenciamento de todas as informações digitais do interesse do Instituto, sejam elas sigilosas ou não, oriundas do IDEFLOR uma vez que deve centralizar todos os dados digitais.

§ 1°. As diretorias/setores irão comunicar ao setor de informática através de memorando os documentos sigilosos e bem como as pessoas autorizadas a acessá-los.

§ 2°. Os servidores autorizados ao acesso de documentos sigilosos assinaram o termo de confidencialidade disposto no anexo 2.

Art. 27. É dever de todo servidor comunicar ao seu superior hierárquico o descumprimento de normas constantes nesta Instrução Normativa.

Art.28. A Diretoria Administrativa e Financeira fará circular permanentemente comunicado para conhecimento desta Instrução Normativa

Art. 29. Esta Instrução Normativa entra em vigor na data de sua publicação no Diário Oficial do Estado.

Thiago valente Novaes
DIRETOR GERAL

ANEXO I
MANUAL DE CONCEITOS

Art. 1º. Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I. Acesso externo – Conexão a um recurso tecnológico a partir de equipamento localizado fora do ambiente informatizado. Geralmente, isso implica o uso de um computador, um modem e algum software de acesso remoto para estabelecer conexão ao servidor de rede;

II. Administrador de sistema – Pessoa que tem a função de gerenciar os sistemas ou parte deles;

III. Ambiente compartilhado – Recurso que permite acesso para mais de um usuário;

IV. Ambiente de desenvolvimento – Conjunto de softwares