NÚMERO DE PUBLICAÇÃO: 401415

INSTRUÇÃO NORMATIVA Nº 01 DE 19 DE JUNHO DE 2012 REGULAMENTA AS NORMAS DE SEGURANÇA EM CUMPRIMENTO ÀS DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE DESENVOLVIMENTO FLORESTAL DO ESTADO DO PARÁ.

O **DIRETOR GERAL,** usando das atribuições que lhe são conferidas por Lei, e tendo em vista a necessidade de normatizar procedimentos de segurança e auditoria de sistemas informatizados e uso de recursos tecnológicos no Instituto de Desenvolvimento Florestal do Estado do Pará,

RESOLVE:
Instituir a política de segurança da informação do Instituto de Desenvolvimento Florestal do estado do Pará

DISPOSIÇÃO PRELIMINAR

Art. 1º. As disposições contidas nesta Instrução Normativa regulamentam a Política de Segurança da Informação do Instituto. Orientam todos os servidores e colaboradores que utilizem o ambiente informatizado Institucional.

CAPÍTULO I
NORMAS GERAIS PARA USUÁRIOS

Art. 2º. Este capítulo determina um conjunto de regras a serem seguidas pelos servidores do Instituto de Desenvolvimento Florestal do Estado do Pará, prestadores de serviço, colaboradores e por todos aqueles que utilizem ou gerenciem o seu ambiente informatizado, a fim de promover a segurança das informações e dos recursos tecnológicos.
§1°. Por ambiente informatizado deste Instituto entende-se todos os seus equipamentos tecnológicos, bem como os sistemas e as informações sob sua responsabilidade e gerência.
§2°. Não são considerados usuários visitantes eventuais.

DOS DEVERES

Art. 3º. É dever do usuário:
I - Conhecer a Política de Segurança da Informação e responsabilizar-se pelo seu cumprimento;
II - Utilizar somente os recursos tecnológicos que lhe forem autorizados, sendo o seu uso limitado aos interesses deste Instituto e para os fins previstos;
III – Ativar proteção de sessão com senha sempre que se ausentar de sua estação de trabalho, se aplicável;
IV - Encerrar sua sessão de trabalho e desligar os equipamentos ao final do período ou do expediente;
V - Zelar pelos equipamentos de informática;
VI - Informar imediatamente ao setor de informática sobre quaisquer problemas ocorridos em equipamentos de informática;
VII - Acompanhar os técnicos de informática quando ocorrer manutenção nas suas estações de trabalho ou nos equipamentos sob sua responsabilidade.
VIII – Manter a segurança dos equipamentos sob sua guarda.

DO USO DA INFORMAÇÃO

Art. 4°. O usuário deve manter sigilo sobre as informações consideradas restritas ou confidenciais, respeitadas as disposições dispostas no Art. 12 e Art. 26 desta Instrução Normativa. Devendo guardá-las de forma protegida, e informar o superior imediato quando informações e/ou aplicações críticas forem encontradas sem tratamento de segurança adequado.
Art. 5°. A impressão de qualquer informação extraída do sistema informatizado é de responsabilidade de quem a emitir ou detiver, proibida qualquer forma de comercialização, divulgação desautorizada ou descarte indevido.

DO ACESSO A SISTEMAS E RECURSOS TECNOLÓGICOS

Art. 6º. Os atos e acessos do usuário às informações e aos recursos tecnológicos devem ser realizados através de senha ou outro dispositivo de identificação.
§ 1°. As senhas de acesso são pessoais e intransferíveis, devem ser mantidas em sigilo e o uso indevido acarretará em seu imediato bloqueio.
§ 2°. O usuário é corresponsável pelos atos cometidos por terceiros com sua senha, seja por ação de empréstimo ou omissão na sua guarda, desde que comprovada culpa ou dolo.
§ 3°. O usuário deve evitar a adoção de senhas frágeis tais como nomes próprios, palavras de vocabulário, siglas, datas comemorativas, dentre outras que possam ser reveladas com facilidade.
§ 4°. É proibida a tentativa, por um usuário não autorizado, de quebrar a segurança do sistema ou descobrir a senha de outros usuários, sob pena de instauração de processo administrativo disciplinar.
§ 5°. A senha de administrador é restrita aos administradores da rede pertencentes ao setor de informática, sendo proibida a sua utilização por outros usuários.

DO USO DE SOFTWARE E HARDWARE

Art. 7º. A utilização de sistemas, programas e equipamentos de informática deve restringir-se às atribuições funcionais do servidor.
§ 1°. A instalação de software, seja na estação do usuário ou no ambiente de rede, somente pode ser procedida ou autorizada pelo setor de informática, sendo proibida a utilização de qualquer programa não autorizado nos equipamentos do Instituto.
§ 2°. A solicitação de aquisição de software imprescinde de parecer técnico do setor de informática.
§ 3°. A cessão de softwares adquiridos de terceiros ou desenvolvidos internamente, para utilização fora do ambiente deste Instituto, somente pode ser realizada após concessão formal do setor de informática, observadas as normas contratuais.
§ 4°. A conexão de equipamentos particulares nas redes internas deve ser autorizada pelo responsável do setor de informática.
§ 5°. É proibido alterar a configuração da estação de trabalho, devendo-se respeitar os padrões de hardware e software implementados.

§ 6º. A manutenção dos equipamentos e sua movimentação física só pode ser efetuada por pessoal da área de informática ou autorizada por ela.

DA INFRAESTRUTURA DE REDE

Art. 8º. A instalação, remanejamento e desinstalação de pontos elétricos e lógicos pertencentes a este Instituto é de competência do setor de informática.
Parágrafo único. É proibido o uso da rede elétrica de computadores para ligação de qualquer equipamento ou utensílio que não seja de informática.

DO USO DA INTERNET E INTRANET

Art. 9º. A Internet e Intranet são disponibilizados tendo em vista os benefícios oferecidos em termos de intercâmbio, pesquisas, estudos e acessos à distância. Todas as regras atuais do Instituto de Desenvolvimento Florestal do Estado do Pará, visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição
com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.
§ 1º. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a Auditoria e divulgação.
Portanto, o Setor de Informática, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.
§ 2º. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Instrução Normativa.
§ 3º.O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.
§ 4º.É proibida a divulgação e/ou o compartilhamento indevido de informações confidenciais do IDEFLOR em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
§ 5º. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
§ 6º.O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos.
§ 7º.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.
§ 8º.Não é permitido acesso a sites de proxy
§ 9º. Qualquer aplicação remota e transmissão de dados somente podem ser disponibilizadas após análise da Informática.
§ 10º. O acesso à internet é configurado no perfil de rede do usuário, sendo este acesso pessoal e intransferível, ficando o usuário responsável por este recurso e pelos atos cometidos por ações ou omissões de empréstimos de acesso.
§ 11º. É considerado uso indevido do recurso o acesso a sites ou qualquer outra atividade em desconformidade com os interesses deste Instituto e das atribuições funcionais do servidor, que degradem a performance dos recursos tecnológicos ou ainda que representem ameaça à segurança.

DO USO DO CORREIO ELETRÔNICO

Art. 10. O sistema de correio eletrônico destina-se a facilitar a comunicação entre os servidores deste Instituto e manter segura as comunicações interinstitucionais.
§ 1º. O usuário deve utilizar o correio eletrônico Institucional em conformidade com os interesses deste Instituto, mantendo suas mensagens restritas ao cumprimento de suas atribuições funcionais.
§ 2º. O Usuário deve sempre remover as mensagens obsoletas e
não mais necessárias, com o objetivo de obedecer a capacidade de arquivos de mensagens estipulada pelo setor de informática.
§ 3º.É proibido aos servidores o uso do correio eletrônico do
Instituto de Desenvolvimento Florestal do Pará, para:
I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
II - enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Instituto de Desenvolvimento Florestal do Pará ou suas unidades vulneráveis a ações civis ou criminais;
IV - divulgar informações não autorizadas ou imagens de tela,
sistemas, documentos e afi ns sem autorização expressa e formal
concedida pelo proprietário desse ativo de informação;
V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
VI - apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do Instituto estiver sujeita a algum tipo de investigação.
VII – enviar ou receber mensagens de cunho pessoal
VIII - produzir, transmitir ou divulgar mensagem que:
a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Instituto;
b) contenha ameaças eletrônicas, como: *spam*, *mail bombing,* vírus de computador;
c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
d) vise obter acesso não autorizado a outro computador, servidor ou rede;
e) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
f) vise burlar qualquer sistema de segurança;
g) vise vigiar secretamente ou assediar outro usuário;
h) vise acessar informações confidenciais sem explícita

autorização do proprietário;
i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
j) inclua imagens criptografadas ou de qualquer forma mascaradas;
k) contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
l) tenha conteúdo considerado impróprio, obsceno ou ilegal;
m) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
n) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
o) tenha fins políticos locais ou do país (propaganda política);
p) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos

DA CÓPIA DE SEGURANÇA E DESCARTE

Art. 11. As informações armazenadas localmente, nas estações de trabalho, são de responsabilidade do usuário.
§ 1°. O usuário deve realizar procedimentos de criação e guarda de cópias de segurança das informações importantes em ambiente seguro, disponibilizado pelo setor de informática, a cada três meses.
§ 2°. O usuário deve manter sempre atualizadas as cópias de segurança.
§ 3°. Informações sigilosas devem estar protegidas por senha ou serem guardadas em local de acesso restrito, previamente solicitado ao setor de informática, ou em dispositivo de armazenamento removível.
§ 4°. O usuário deve remover do ambiente informatizado, de forma irrecuperável e seguindo orientações do setor de informática, os arquivos e informações que não sejam mais necessários
§ 5°. Os documentos impressos extraídos dos sistemas devem ser destruídos definitivamente quando não forem mais necessários.

DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art.12. Para garantir as regras mencionadas nesta Instrução Normativa, o Instituto de Desenvolvimento Florestal poderá:
I . Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede
II . A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
III. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria do setor de informática, no caso de exigência judicial, solicitação do gerente (ou superior).
IV. Realizar, a qualquer tempo, inspeção física nas máquinas de propriedade do Instituto;
V. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
§ 1°. O usuário não poderá utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
§ 2°. O usuário não poderá apropriar-se para si ou para outrem de material confidencial e/ou sigiloso de produção intelectual ou decorrente do uso da tecnologia que venha a ser disponível;
§ 3º. Cada setor será responsável por informar ao setor de informática através de memorando os documentos sigilosos e bem como as pessoas autorizadas a acessá-los

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.
§ 5º. 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 reprocessamento 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.
§ 1º. É necessário que se preserve a compatibilidade com o ambiente operacional e físico da época da geração da cópia de segurança.
§ 2º. 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.
§ 3º. 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.
§ 1º. Esse registro não exclui outros necessários ao controle de patrimônio.
§ 2º. Cabe ao setor de informática local a movimentação interna de equipamentos bem como sua instalação e configuração, devidamente documentadas.
§ 3º. 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.
§ 1º. O acesso a esse ambiente deve ser restrito apenas aos técnicos e administradores responsáveis pelos equipamentos.
§ 2º. Deve haver controles que garantam temperatura adequada, além de outros que visem proteger o equipamento contra quaisquer ameaças.
§ 3º. 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.
§ 1º. 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.
§ 2º. Cabe aos responsáveis pelos processos críticos elaborar os planos e coordenar a sua execução.
§ 3º. Devem ser implementadas rotinas de teste dos planos de contingência com o objetivo de avaliar sua eficácia.
§ 4º. Cada plano de contingência deve estar difundido entre os responsáveis por sua execução e suas chefias.
§ 5º. O conjunto dos Planos de Contingência dos recursos críticos compõe o Plano de Continuidade de Negócio, que será homologado pelo Núcleo da Informação (informática).
§ 6º. 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.
§ 1º. Cabe a Informática realizar auditoria nos sistemas e procedimentos executados pelo próprio Setor.
§ 2º. Deve constar dos procedimentos de auditoria a sua periodicidade, forma de verificação e sua duração.
§ 3º. 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.
§ 1º. As diretorias/setores irão comunicar ao setor de informática através de memorando os documentos sigilosos e bem como as pessoas autorizadas a acessá-los.
§ 2º. 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 e dados fictícios utilizados para construção e teste dos sistemas em desenvolvimento;
V. Ambiente de produção – Conjunto de softwares e dados reais em uso pela organização;
VI. Ambiente de rede – Área de compartilhamento de recursos tecnológicos;
VII. Ambiente informatizado – Conjunto dos equipamentos, sistemas e informações de uma organização;
VIII. Ambiente operacional - Ambiente lógico composto de software e controlado por sistemas operacionais;
IX. Antivírus - Software que identifica e remove vírus de computador;
X. Aplicação crítica - Aplicação que atualiza valores, concede autorizações de acesso e/ou trata de informações sigilosas ou vitais para a execução das atividades deste Instituto;
XI. Aplicativo – Programa desenvolvido internamente ou por empresa de software para uso em alguma aplicação específica;
XII. Backup - Um substituto ou alternativa para um recurso. O termo backup refere-se, usualmente, a um disco ou fita que contém uma cópia de segurança;
XIII. Código executável – Código em linguagem de computador pronto para ser executado;
XIV. Código fonte – Texto desenvolvido por programadores que instruem o computador para a realização de alguma tarefa;
XV. Colaboradores – Entidades públicas ou privadas ligadas à este Instituto para compartilhamento de informações ou serviços;
XVI. Confidencialidade/sigilo – Permissão de acesso à informações apenas aos usuários autorizados. Varia de acordo com a gravidade do impacto que a revelação não autorizada traz para a organização;
XVII. Configuração - Conjunto dos componentes internos e externos de um recurso tecnológico;
XVIII. Cópia de segurança - Disco ou fi ta que contém uma cópia de informações com o intuito de recuperá-las em caso de perda ou modificação indevida;
XIX. Correio eletrônico - Serviço de comunicação que consiste na troca de mensagens eletrônicas através de redes de computadores. Mesmo que e-mail;
XX. Criptografia - Técnica utilizada para converter uma informação num código secreto, com propósitos de segurança, para que não possam ser utilizadas ou lidas até serem decodificadas;
XXI. Descarte indevido – inutilização ou destruição de informação sem o devido tratamento para que essa informação não possa mais ser aproveitada;
XXII. Disponibilidade – Grau de exigência que a informação possui em estar acessível. Varia de acordo com a gravidade do impacto que a indisponibilidade da informação traz para a organização;
XXIII. Dispositivo de armazenamento removível – Artefato portátil utilizado para gravar dados;
XXIV. Estação de trabalho - Refere-se a qualquer computador conectado a uma rede;
XXV. Ferramentas – Programas de computador destinados a gerenciar o ambiente informatizado;
XXVI. Gestor de recurso tecnológico – Pessoa responsável pela gerência de equipamento ou sistema informatizado;
XXVII. Hardware – Equipamento físico ou dispositivos mecânicos, elétricos ou eletrônicos, que compõem os equipamentos computacionais;
XXVIII. Indicadores – Dados coletados para fins de análise;
XXIX. Informação - É todo conhecimento a respeito de algo ou alguém, gerado por algum evento, mantido armazenado em algum meio, consultado e/ou modificado por ação de agentes
competentes, e que é instrumento de trabalho fundamental para
o funcionamento de qualquer organização;
XXX. Informação crítica - Informação sigilosa ou vital para a execução das atividades deste Instituto;
XXXI. Integridade - Capacidade efetiva da informação estar intacta e garantida contra perda, dano ou modificação não autorizada;
XXXII. Internet - Rede de computadores de alcance mundial conectados entre si;
XXXIII. Intranet - Rede de computadores de alcance restrito aos equipamentos deste Instituto;
XXXIV. Perfil de acesso – Conjunto de permissões atribuídas aos usuários de um sistema;
XXXV. Perfil de rede – Acessos disponíveis através do usuário do ambiente de rede;
XXXVI. Plano de Contingência – É o conjunto de procedimentos que descrevem os passos para a recuperação de um recurso tecnológico em caso de problemas de funcionamento;
XXXVII. Plano de Continuidade de Negócios – É o conjunto de Planos de Contingência que se complementam a fim de oferecer uma solução completa para a continuidade de negócios em caso de interrupção das atividades;
XXXVIII. Prestador de serviço – Funcionário ou empresa contratada pelo IDEFLOR para realização de atividades permanentes ou com prazo de conclusão;
XXXIX. Processos, equipamentos e recursos críticos – Meios pelos quais as informações tramitam e que são vitais para a execução das atividades do IDEFLOR;
XL. Programa – Conjunto de comandos que instruem o computador a realizar uma tarefa. Ver software.
XLI. Proteção de sessão – Programa que protege a sessão de trabalho do usuário contra a sua utilização por outras pessoas em caso de inatividade da estação de trabalho durante o seu funcionamento.
XLII. Publicidade ou transparência – Indica que os atos da administração devem merecer a mais ampla divulgação possível entre os administrados, e isso porque constituem fundamento do princípio, propiciar-lhes a possibilidade de controlar a legitimidade da conduta dos agentes administrativos, é com a transparência que poderão os indivíduos aquilatar a legalidade ou não dos atos e o grau de sua eficiência.
XLIII. Recurso tecnológico – Qualquer equipamento ou sistema informatizado;
XLIV. Roteador – Equipamento destinado a direcionar o tráfego entre redes de computadores;
XLV. Senha - Uma série secreta de caracteres que habilita um usuário para acesso a um recurso tecnológico;
XLVI. Servidor (equipamento) – Computador que, numa rede local, administra serviços disponíveis a outros computadores;
XLVII. Servidor fazendário – Funcionário do Instituto investido em cargo publico, contratado, cedido de outro órgão ou em regime de prestação de serviço;
XLVIII. Sessão de trabalho – É o intervalo de tempo em que um sistema está autenticado para um usuário;

XLIX. Sistema informatizado - Conjunto de várias funções interligadas que automatiza um processo;
L. Sites – Conteúdo disponível na rede mundial de computadores através de páginas identificadas por endereços eletrônicos;
LI. Sites proibidos – São categorias de sites que agridem os bons costumes, que prejudicam as atividades do funcionário ou comprometem a eficiência dos recursos de tráfego de dados;
LII. Software - Conjunto de programas, procedimentos, regras e documentação referentes à operação de um sistema, armazenado eletronicamente;
LIII. Spam – Correspondência eletrônica enviada para diversos destinatários sem o consentimento dos mesmos.
LIV. Uso indevido – Utilização dos recursos tecnológicos em desconformidade com as atribuições funcionais.
LV. Usuário - Qualquer pessoa que utiliza recursos tecnológicos;

ANEXO II

Termo de Confidencialidade e Sigilo – OUTROS e IDEFLOR

_____, (nacionalidade), (estado civil), (profissão), inscrito (a) no CPF sob o nº. _____, abaixo firmado, assume o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas e outras relacionadas ao desenvolvimento da tecnologia "_____ ", a que tiver acesso durante a apresentação realizada pelo (a) servidor(a) _____, no dia _____/_____/_____, nas dependências do departamento
de _____, Instituto de Desenvolvimento Florestal do Pará – Ideflor.
Por este Temo de Confidencialidade e sigilo compromete-se:
1. a não utilizar as informações confidenciais contidas na apresentação a que tiver acesso, para gerar beneficio próprio exclusivo e / ou unilateral, presente ou futuro, ou para uso de terceiros;
2. a não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso durante a apresentação da tecnologia acima mencionada;
3. a não apropriar-se para si ou para outrem de material confidencial e/ ou sigiloso que venha a ser disponível pela apresentação da tecnologia ora mencionada;
4. a não repassar o conhecimento das Informações confidenciais, responsabilizando-se por todos as pessoas que vierem a ter acesso às informações, por intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.
Neste Termo, as seguintes expressões serão assim definidas:
"Informação Confidencial": significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.
"Informação Confidencial": inclui, mas não se limita, à informação relativa às operações, processos planos ou intenções, informações sobre produção, instalações, equipamentos, segredos de negócios, segredos de fábrica, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especificações, componentes, formulas, produtos, amostras, diagramas, desenhos de esquema industrial, patentes, oportunidades de mercado e questões relativas a negócios revelados na apresentação da tecnologia supramencionada.
"Avaliação": significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a apresentação da tecnologia XX acima mencionada.
A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.
Pelo não cumprimento do presente Termo de Confidencialidade e sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Belém, _____de _____ de _____

_____
Nome
CPF