ESTADO DO CEARÁ
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
ASSESSORIA DE POLÍTICAS INSTITUCIONAIS

PROVIMENTO Nº 82/2013

Institui a Política de Segurança da Informação no âmbito do Ministério Público do Estado do Ceará e dá outras providências.

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO CEARÁ, no uso das atribuições legais lhe conferidas pelo art. 127, § 2º, da Constituição Federal c/c o art.10, inciso V, da Lei Federal nº 8.625, de 12 de fevereiro de 1993 e disposições contidas no art. 26, V, XVIII e XXXIII da Lei Complementar Estadual nº 72, de 12 de dezembro de 2008 – Lei Orgânica e Estatuto do Ministério Público do Estado do Ceará,

CONSIDERANDO que a Constituição Federal assegura ao Ministério Público autonomia funcional e administrativa, permitindo-lhe praticar atos próprios de gestão, incluindo a expedição de provimento para disciplinar as atividades administrativas do órgão;

CONSIDERANDO a atual intensidade de fluxo de dados, informações, conhecimentos, documentos, materiais e demais assuntos que tramitam pelo Ministério Público cotidianamente;

CONSIDERANDO a necessidade de se criarem normas de proteção da informação com o escopo de evitar vulnerabilidades e incidentes de segurança no âmbito deste Ministério Público;

EXTRATO

CONSIDERANDO a imperiosidade de se preservar o sigilo, integridade, disponibilidade, uso e valor dos dados e informações eletronicamente armazenados;

CONSIDERANDO a importância de desenvolver uma cultura de segurança da informação entre os membros, servidores e demais colaboradores da instituição;

CONSIDERANDO que a referida salvaguarda requer conhecimento, cultura e conduta de segurança, além da adoção de procedimentos cautelares específicos, os quais devem ser conhecidos e executados por todas as pessoas que tratam ou que, por qualquer meio, tenham acesso aos referidos assuntos ou contatos com estes;

CONSIDERANDO a necessidade da consolidação de uma política de segurança da informação no âmbito do MP/CE;

CONSIDERANDO a criação do Núcleo de Inteligência e Segurança Institucional do Ministério Público, instituído por meio do Provimento nº 95/2010, com a finalidade de produzir conhecimento para a tomada de decisões estratégicas;

CONSIDERANDO a Recomendação nº 13, de 16 de junho de 2009, do Conselho Nacional do Ministério Público, que determina a criação de um Plano de Segurança Institucional nos campos de segurança da informação, recursos humanos, materiais, áreas e instalações;

CONSIDERANDO a necessidade de se adequar a Política de Segurança da Informação conforme os ditames e as alterações introduzidas pela Lei nº 12.527/2011 (Lei de Acesso à Informação);

CONSIDERANDO os princípios constitucionais da legalidade, publicidade e eficiência, que norteiam a Administração Pública, nos termos da Constituição Federal;

CONSIDERANDO, enfim, as disposições contidas no procedimento administrativo nº 15872/2010-2;

RESOLVE editar o seguinte Provimento:

Art. 1º. Fica criada e instituída a Política de Segurança da Informação, conforme Anexos.

Art. 2º. O Procurador-Geral de Justiça editará atos necessários para a operacionalização das diretrizes, ações e normas contidas na Política de Segurança da Informação.

Art. 3º. A difusão da Política de Segurança da Informação do Ministério Público do Estado do Ceará será realizada gradativamente, observadas as condições orçamentárias.

Art. 4º. Compete à Secretaria de Tecnologia da Informação editar, exclusiva ou conjuntamente com outros órgãos, Plano de Atuação para detalhamento das ações de execução da Política de Segurança da Informação.

Art. 5º. A Política de Segurança da Informação, contida nos Anexos, deverá ser difundida no âmbito do Ministério Público do Estado do Ceará.

Art. 6º. Por medida de segurança, estrategicamente, o Plano de Atuação de Segurança da Informação não deverá ser tornado ostensivo, por força da classificação que lhe for atribuída, devendo ser publicado sob a forma de extrato, o qual não comprometerá seu conteúdo, que estará disponível aos membros e servidores, no prazo de 30 (trinta) dias.

Art. 7º. As disposições, os princípios e as diretrizes previstas na Política de Segurança da Informação possuem natureza obrigatória, de modo que o seu descumprimento poderá acarretar sanções previstas no ordenamento jurídico pátrio.

Art. 8º. Este Provimento entra em vigor na data de sua publicação, revogando-se as disposições contrárias.

Registre-se. Publique-se. Cumpra-se.

Gabinete do Procurador-Geral de Justiça, em Fortaleza, 12 de abril de 2013.

Alfredo **RICARDO** Cavalcante de Holanda **MACHADO**
Procurador-Geral de Justiça do Estado do Ceará

Ministério Público do Ceará
Procuradoria Geral de Justiça
Secretaria Geral
Secretaria de Tecnologia da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

1. Apresentação

A Secretaria de Tecnologia e Informática, em sua atribuição institucional de Coordenação Técnica da Informática, responsável por propor e prover soluções de Tecnologia da Informação tem como incumbência a elaboração de uma Política de Segurança da Informação do setor de Informática e Comunicações, com o objetivo de normatizar, padronizar e estabelecer requisitos mínimos, a fim de proporcionar condições que assegurem a integridade, a confidencialidade e a disponibilidade da informação no âmbito de seu ambiente computacional.

Este documento tem como propósito definir a política de segurança da informação e comunicações de acordo com as normas da Política de Segurança Institucional e o Plano de Segurança Institucional do Ministério Público do Ceará.

2. Objetivo

Este documento tem como objetivo definir normas de segurança com definições, diretrizes, restrições e requisitos a serem aplicados aos ambientes computacionais do Ministério Público do Ceará de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, descrevendo procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

3. Abrangência da Segurança

Deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes no Ministério Público do Ceará como também às atividades de todos os servidores, colaboradores internos e externos, estagiários e prestadores de serviço que exercem atividades no Ministério Público do Ceará ou a quem quer que venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

4. Terminologia

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

5. Conceitos e Definições

Aplicam-se os conceitos abaixo no que se refere à Política de Segurança da PGJ.

I - ***Ativo de Informação*** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades;

II - ***Ativo de Processamento*** – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos;

III - ***Controle de Acesso*** – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

IV - ***Custódia*** – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia

não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

V - ***Direito de Acesso*** – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

VI - ***Ferramentas*** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades;

VII - ***Incidente de Segurança*** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da PGJ;

VIII - ***Política de Segurança*** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

IX - ***Proteção dos Ativos*** – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

X - ***Responsabilidade*** – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

XI - ***Senha Fraca ou Óbvia*** – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

6. Diretrizes da Política de Segurança

A presente Política de Segurança da Informação e Comunicações engloba diversos aspectos físicos, lógicos e de pessoal que, por suas extensões e particularidades, serão detalhadas isoladamente como normas, padrões e requisitos específicos de segurança, devendo compor este documento principal na forma de anexos.

6.1 Gestão de Segurança

6.1.1 Esta Política de Segurança deve abranger todos os recursos humanos, administrativos e tecnológicos do Ministério Público do Ceará;

6.1.2 Deve existir programa de disseminação desta Política assegurando que todos que integram a Instituição estejam cientes da obrigatoriedade de obediência às normas e recomendações aqui definidas. Para tanto, esta Política de Segurança encontra-se disponível no site e na intranet da PGJ;

6.1.3 Deve ser implementado um programa de conscientização sobre Segurança da Informação de forma que todos sejam informados sobre os potenciais riscos de segurança a que estão expostos os ambientes computacionais, proporcionando, assim, maior cooperação para o cumprimento das normas desta Política;

6.1.4 Devem existir procedimentos específicos documentados para bloqueio temporário ou definitivo de acesso aos sistemas, recursos e serviços computacionais da PGJ quando do afastamento ou desligamento de usuários credenciados;

6.1.5 Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários quando da utilização dos sistemas, recursos e serviços computacionais do Ministério Público do

Ceará, ficando os transgressores sujeitos às sanções administrativas, civis e penais;

6.1.6 O uso de recursos computacionais particulares no âmbito da PGJ é permitido apenas mediante a autorização prévia do gestor responsável e, somente, após auditoria quanto à conformidade com as normas de segurança desta Política, pelo gestor de segurança;

6.1.7 Documentos e softwares desenvolvidos por funcionários e prestadores de serviço são de propriedade da PGJ, ressalvados os casos expressamente assegurados em contrato ;

6.1.8 A identificação do usuário por meio de crachá, senha ou outro meio é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso de qualquer uma dessas formas de identificação, a assinatura de "Termo de Responsabilidade", que comprove sua ciência às condições de uso, seus direitos e deveres quanto ao acesso dos recursos computacionais da PGJ;

6.1.9 Todas as informações devem ser protegidas contra perda, acessos e usos indevidos, devendo ser adotados procedimentos específicos e adequados ao grau de criticidade da informação, que estão sob a responsabilidade direta do funcionário ou prestador de serviço;

6.1.10 Os recursos de processamento da informação disponibilizados aos usuários devem ser planejados e projetados a fim de evitar situações de risco à segurança da informação e devem ser homologados em ambiente próprio antes de serem postos em ambiente de produção;

6.1.11 Todos os usuários ao tomarem conhecimento de qualquer incidente de Segurança da Informação devem notificar o fato imediatamente a Secretaria de Tecnologia e Informática - STI, para as providências cabíveis;

6.1.13 Todos os usuários, funcionários, terceirizados e prestadores de serviço em geral devem ter acesso permitido apenas aos recursos necessários à execução de suas tarefas no âmbito do Ministério Público do Ceará, de forma a evitar vulnerabilidades;

6.2 Gerenciamento de Riscos

6.2.1 Deve ser implementado até 180 dias contados da publicação desta Política de Segurança da Informação, sob a responsabilidade da Secretaria de Tecnologia e Informática e do gestor de segurança, um programa de gerenciamento de riscos para análise do ambiente computacional da PGJ com objetivo de identificar e remediar as vulnerabilidades que resultam em riscos para a segurança das informações;

6.2.2 A Análise de Risco deve ser feita pelo menos uma vez ao ano, emitindo relatório para apresentação e análise junto à Diretoria e aos demais Gestores;

6.2.3 Os riscos a serem avaliados compreendem, dentre outros, os seguintes:

Segmento	**Riscos**
Dados e Informação	Indisponibilidade, Interrupção (perda), interceptação,modificação, fabricação, destruição
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, perda de conhecimento
Rede	*Hacker*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço.

Hardware	Indisponibilidade, interceptação (furto ou roubo), falha
Software e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento, falha.
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, hardware criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico.

6.3 Plano de Continuidade de Negócio

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos da PGJ na eventualidade da ocorrência de desastres, atentados, falhas e intempéries;

6.3.1 Um plano de continuidade do negócio deve ser implementado e testado periodicamente para garantir a continuidade dos serviços críticos nos ambientes computacionais;

6.3.2 Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos quando necessário;

6.3.3 Procedimentos específicos devem ser implementados em até 180 dias contados da publicação desta Política de Segurança da Informação para contingência nas diversas áreas de atuação dos ambientes computacionais, cabendo aos respectivos gestores, tomarem as providências cabíveis;

7. Documentos Referenciados.

Conforme explicado anteriormente, os aspectos de segurança física, lógica e de pessoal, serão tratados em documentos independentes, tendo em vista suas peculiaridades e deverão compor este documento principal da Política de Segurança da Informação e Comunicações na forma de anexos, a fim de complementar com maior especificidade e detalhamento, as normas e recomendações de segurança no trato das informações.

Abaixo, segue a relação das demais normas de segurança que serão detalhadas como anexos:

a. Norma sobre o uso do correio eletrônico.
b. Norma sobre o acesso a Internet.
c. Norma de Segurança sobre desenvolvimento de sistemas e serviços.
d. Norma de segurança do Ambiente Lógico
e. Norma de segurança do Ambiente Físico.

8. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.

Ministério Público do Ceará
Procuradoria Geral de Justiça
Secretaria Geral
Secretaria de Tecnologia da Informação

Anexo I

Norma do uso da Internet

1. Apresentação

Considerando que o uso dos serviços de aceso a Internet, no âmbito do Ministério Público do Ceará, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico. Todos os Usuários desse serviço deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de uso da Internet no âmbito do Ministério Público do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança Institucional do Ministério Público do Ceará e Política de Segurança da Informação e Comunicações do Ministério Público do Ceará.

4. Definições

I - Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];

II - Software – Programa de Computador;

III - Download – Baixar um arquivo ou documento de outro computador, através da Internet;

IV - Upload – Envio de um arquivo de seu computador para outro, através da Internet;

V - Peer-to-Peer (P2P) – É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet;

VI - URL - Universal Resource Locator - LINK ou endereço de uma página Web, como por exemplo http://www.mp.ce.gov.br;

VII - Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários;

VIII - Códigos Maliciosos ou Agressivos – Qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico;

IX - Código de Acesso – Código de acesso atribuído a cada Usuário. A cada código de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos computacionais disponíveis;

X - Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

5. Procedimentos referentes ao uso do acesso à Internet.

5.1. Criação/Exclusão de conta de acesso à Internet

5.1.1 Para Obter o acesso à Internet:

5.1.1.1 A chefia imediata deverá solicitar à Secretaria de Tecnologia e Informática, por meio de memorando assinado ou mensagem eletrônica para informatica@mp.ce.gov.br informando: nome completo do usuário, setor/órgão de lotação, matrícula e justificativa da necessidade da conta de acesso à Internet;

5.1.1.2 A Secretaria de Tecnologia e Informática efetuará o procedimento e informará ao interessado a sua credencial e Normas de uso da Internet;

5.1.1.3 A credencial deve ser confidencial e não compartilhada. O gestor imediato será responsável pelas contas de acesso à Internet pertencentes ao seu setor;

5.1.2 Para Excluir o acesso à Internet:

5.1.2.1 O gestor imediato deverá solicitar à Secretaria de Tecnologia e Informática, por meio de memorando assinado ou mensagem eletrônica, informando o nome completo do usuário, setor de lotação e matrícula;

5.1.2.2 Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar à Secretaria de Tecnologia e Informática para que o remanejamento do usuário seja realizado;

5.2 Regras Gerais

5.2.1 O acesso à Internet, no âmbito do Ministério Público do Ceará, é uma concessão e não um direito. Portanto a sua utilização deve ser para atividades inerentes aos trabalhos desenvolvidos;

5.2.2 O acesso à Internet é feito unicamente pela conexão provida pelo órgão, ficando proibida a utilização diferente desta;

5.2.3 Todas as contas de acesso à Internet terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

5.2.4 O acesso à Internet será monitorado por meio de ferramentas próprias, podendo os acessos serem auditados quando necessário. Todos os registros de acessos à Internet são passíveis de auditoria;

5.2.5 É expressamente proibido o acesso à Internet para violar leis e regras brasileiras ou de qualquer outro país. O uso dos recursos de Internet providos pelo Ministério Público do Ceará para atividades ilegais é razão para perda de privilégios e sanções cabíveis;

5.2.6 Somente usuários autorizados a falar, analisar ou publicar documentos em nome do Ministério Público do Ceará poderão fazê-los em comunicações eletrônicas;

5.2.7 O Ministério Público do Ceará mantém o direito de cópia de todo material postado na Internet por qualquer usuário no curso de suas obrigações;

5.2.8 São consideradas como práticas não aceitáveis para acesso à Internet site de: racismo, terrorismo, hacker, assédio sexual, pornografia, pedofilia, incentivo a violência, descriminação, bate-papo, sites de relacionamento, redes sociais, jogos, rádio, músicas, tv online, vírus e outros não condizentes com os

objetivos institucionais do Ministério Público, salvo casos onde executado por usuário autorizado para coleta de dados que promovam a tentativa de elucidação de casos de evidência de autoria ou acessos e para o fornecimento de elementos de prova em processos judiciais;

5.2.9 Os usuários da Internet somente deverão realizar downloads de grandes arquivos (acima de 10Mb) fora do horário de expediente, para não comprometer o funcionamento da infraestrutura de computação do Ministério Público do Ceará;

5.2.10 É proibida a divulgação de informações sigilosas da Instituição em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, ficando aquele que assim proceder, sujeito às penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

5.2.11 Usuários com acesso à Internet não podem efetuar *upload* de qualquer *software* licenciado pela Instituição ou de dados de propriedade institucional ou de seus membros e servidores, sem a expressa autorização do gerente responsável;

5.2.12 Caso o Ministério Público do Ceará julgue necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do usuário, bem como, que exponham a rede a riscos de segurança;

5.2.13 É proibido adotar de forma independente da Secretaria de Tecnologia e Informática, quaisquer mecanismos de codificação/criptografia;

5.2.14 Se algum usuário souber de qualquer violação a esta Norma deverá comunicar ao setor competente da Secretaria de Tecnologia e Informática e a sua chefia imediata;

5.3 Deveres, Responsabilidades e Recomendações

5.3.1 Deveres do Usuário

5.3.1.1 Utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos, a ordem pública e as definições desta Norma;

5.3.1.2 Evitar utilizar a Internet, para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, como também danificar e/ou sobrecarregar os recursos tecnológicos (hardware e software);

5.3.1.3 Quando preencher um formulário ou enviar informações confidenciais por meio da Internet deve certificar-se que a conexão está segura através do símbolo do cadeado fechado (SSL) que aparece no canto inferior direito do navegador e da palavra HTTPS substituindo a palavra HTTP na barra de endereço , para certificar que os dados estão sendo enviados de forma segura pela Internet;

5.3.1.4 Desconectar-se imediatamente de um site que contenha acesso restrito, mesmo que tenha sido aceito pelos sistemas encarregados de barrá-lo;

5.3.1.5 Evitar advogar causas políticas e de emitir informações não autorizadas sobre quaisquer serviços, produtos, contextos políticos, dentre outros na Internet;

5.3.2. Responsabilidades do Usuário

5.3.2.1 O usuário é o responsável pelos acessos à Internet realizados pela sua conta;

5.3.2.2 O mau uso de uma conta de acesso à Internet por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;

5.3.2.3 Zelar pelo fiel cumprimento ao estabelecido nesta Norma;

5.3.3 Responsabilidades do Administrador

5.3.3.1 Implantar a autenticação de todos os acessos à Internet;

5.3.3.2 Implantar mecanismos de monitoramento dos acessos à Internet;

5.3.3.4 Arquivar todas as solicitações de acesso à Internet para controle;

5.3.3.5 Adotar mecanismos de criptografia/codificação para transferência de informações sensíveis pela Internet;

5.3.3.6 Verificar periodicamente os acessos à Internet, para detectar eventuais problemas que possam estar ocorrendo;

5.3.3.7 Fornecer, quando solicitado pela direção, relatório de acessos dos usuários;

5.3.3.8 Utilizar o browser padrão Internet Explorer e prover mecanismos de atualizações e correções de segurança;

5.3.3.9 Bloquear sites que vão de encontro a esta Norma e que estejam comprometendo o bom funcionamento dos recursos de Internet;

6. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.

Ministério Público do Ceará
Procuradoria Geral de Justiça
Secretaria Geral
Secretaria de Tecnologia da Informação

ANEXO II
Norma do uso do Correio Eletrônico (e-mail)

1. Apresentação

Esta Norma define a política sobre o uso do Correio Eletrônico no Ministério Público do Ceará e estabelece as diretrizes básicas a serem seguidas pelos usuários e administradores dessa ferramenta, com vistas a assegurar a prioridade de sua destinação às finalidades institucionais.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico no âmbito do Ministério Público do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança Institucional do Ministério Público do Ceará e Política de Segurança da Informação e Comunicações do Ministério Público do Ceará.

4. Definições

I - Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];

II - Caixa Postal/Correio eletrônico – Espaço em disco, onde são armazenadas as mensagens de correio eletrônico;

III - Correio Eletrônico – Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;

IV - Criptografia – Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações;

V - FTP (File Transfer Protocol) – Protocolo padrão da Internet, usado para transferência de arquivos entre computadores;

VI - IMAP (Internet Message Access Protocol) – Protocolo de acesso a mensagens eletrônicas;

VII - Internet – Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc;

VIII - Intranet – Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos Órgãos Públicos;

IX - Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas;

X - POP (Post Office Protocol) – Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico;

XI - Servidor de Correio Eletrônico – Equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico;

XII - SMTP (Simple Mail Transfer Protocol) – Protocolo de comunicação usado para troca de mensagens na Internet, via correio eletrônico;

XIII - Spam – Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado;

XIV - Usuários – Funcionários, prestadores de serviços, clientes,fornecedores, bolsistas e estagiários;

XV - Vírus Eletrônico – São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos;

5. Abrangência

Esta norma deverá ser aplicada aos ativos de informação e comunicação do Ministério Público do Ceará.

6. Vigência

Esta Norma passa a vigorar a partir da data de sua aprovação e será revisada anualmente. A antecipação do processo de revisão poderá ocorrer pela necessidade de reestruturação dos processos administrativos/operacionais do Ministério Público do Ceará.

7. Procedimentos

7.1. Criação/Exclusão de conta de e-mail

7.1.1 Para Obter uma conta de e-mail:

7.1.1.1 A chefia imediata deverá solicitar à Secretaria de Tecnologia e Informática, por meio de memorando ou e-mail, informando: nome completo do usuário, setor de lotação, matrícula e justificativa da necessidade da conta de e-mail;

7.1.1.2 O setor de TI efetuará o cadastro e informará ao interessado: o seu usuário, senha padrão/provisória e Normas de uso do e-mail;

7.1.1.3 O gestor imediato será responsável pelas contas de email pertencentes ao seu setor;

7.2 Para Excluir uma conta de e-mail:

7.2.1 O gestor imediato deverá solicitar à Secretaria de Tecnologia e Informática, através de memorando ou e-mail, informando: nome completo do usuário, setor de lotação e matrícula;

7.2.2 Quando da mudança de setor/órgão ou desligamento, o gestor imediato deverá comunicar a Secretaria de Tecnologia e Informática para que o remanejamento do usuário seja realizado;

7.2.3 Os usuários que estiverem utilizando conta de e-mail de forma inadequada (conforme política de e-mail) terá sua conta inicialmente bloqueada e será comunicado ao seu gestor imediato para adoção das medidas cabíveis;

8. Regras Gerais

8.1 Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

8.2 Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, a critério do titular de Área/Gerência, enquanto perdurar o seu vínculo com a Autarquia;

8.3 Contas com inatividade por um período igual ou superior a 90 (noventa) dias serão bloqueadas após a comunicação com o proprietário da conta informando do bloqueio da mesma, a fim de evitar o recebimento de novas mensagens;

8.4 O tamanho das caixas postais será de 1GB para os usuários membros e gestores e de 800MB para os demais usuários;

8.5 Para fins legais de auditoria, o Ministério Público do Ceará se reserva ao direito de realizar investigações nas caixas postais do e-mail institucional;

9. Deveres, Responsabilidades e Recomendações

Deveres do Usuário

9.1 Não enviar mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade do Ministério Público do Ceará;

9.2 Não utilizar o e-mail do órgão para assuntos pessoais;

9.3 Adotar o hábito de leitura dos e-mails diariamente;

9.4 Enviar e-mails apenas para destinatários que realmente precisam da informação;

9.5 Todo e-mail que possua conteúdo considerado sigiloso deverá ser enviado utilizando criptografia;

9.6 Não fazer acesso, quando não autorizado, à caixa postal de outro usuário;

9.7 Não enviar, armazenar e manusear material que contrarie o disposto nesta política, na legislação vigente, a moral,os bons costumes e a ordem pública;

9.8 Não enviar, armazenar e manusear material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei, proibidos pela Política de Segurança Institucional ou pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware e software*), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

9.9 Não enviar, armazenar e manusear material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

9.10 Não deve utilizar o sistema de correio para envio de mensagens do tipo "corrente";

9.11 Não utilizar as listas e/ou caderno de endereços do Ministério Público do Ceará ou de qualquer Órgão

para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;

9.12 Não usar contas particulares, através dos serviços Post Office Protocol - POP, Internet Message Access Protocol – IMAP e Simple Mail Transfer Protocol - SMTP de provedores não pertinentes aos domínios mp.ce.gov.br;

9.11 Não enviar e-mail com arquivos anexos que comprometam a banda passante do link de comunicação, ou que perturbe o bom andamento dos trabalhos, ou ainda, exponha a rede a riscos de segurança;

9.12 É proibido forjar qualquer das informações do cabeçalho do remetente;

9.13 Deve evitar todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa o Órgão;

9.14 Responsabilidades do Usuário

9.14.1 O usuário é o responsável pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

9.14.2 O mau uso de uma conta de correio por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;

9.14.3 É de exclusiva responsabilidade do usuário o conteúdo de seus arquivos;

9.15 Responsabilidades do Administrador do Correio

9.15.1 Verificar periodicamente a conta postmaster, para detectar eventuais problemas que possam estar ocorrendo no servidor e na entrega de e-mail dos usuários;

9.15.2 Criação das contas "security" e "abuse" nos servidores de domínio;

9.15.2 Implementar o papel de moderador nas listas, como objetivo de evitar spans;

9.16. Recomendações para o Administrador do Correio

9.16.1 Configurar o servidor de correio para enviar e-mail só após a autenticação do Usuário, utilizando configurações do tipo "smtp auth", "smtp after pop", etc;

9.16.2 Utilizar criptografia para o uso do protocolo SMTP, POP e IMAP;

9.16.3 Implementar medidas para filtragem de vírus no sistema de correio eletrônico;

9.16.4 Implementar medidas para filtragem de spam e e-mails indesejados (correntes, mensagens pornográficas, propaganda, etc.) no sistema de correio eletrônico;

9.16.5 Arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) e outras extensões comumente utilizadas por vírus devem ser automaticamente bloqueadas;

9.16.6 Monitorar o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede etc;

10. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.

ANEXO III
Norma sobre o Desenvolvimento e Manutenção de Sistemas.

1. Apresentação

Esta Norma define normas sobre o desenvolvimento de sistemas dentro do Ministério Público do Ceará e estabelece as diretrizes básicas a serem seguidas pelos usuários e desenvolvedores, com vistas a assegurar a prioridade de sua destinação às finalidades institucionais do Ministério Público do Ceará.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de segurança ao ambiente lógico no âmbito do Ministério Público do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança Institucional do Ministério Público do Ceará e Política de Segurança da Informação e Comunicações do Ministério Público do Ceará.

4. Definições

I - Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];

II - Software – Programa de Computador;

III - Ambiente lógico - Todo o ativo de informações das entidades;

IV - Ativo de Informação – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades;

V - Ativo de Processamento – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos;

VI - Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

VII - Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

VIII - Direito de Acesso – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

IX - Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PS da Informação das entidades;

X - Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da PGJ;

XI - Política de Segurança – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

XII - Proteção dos Ativos – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

XIII - Responsabilidade – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

XIV - Senha Fraca ou Óbvia – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

XV - Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

XVI - Proprietário do ativo – Identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo. [ISO/IEC 13335-1:2004 Item 7.1.2] ;

XVII - Usuários – Funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários;

5. Diretrizes Gerais.

5.1 Deverá existir uma metodologia de desenvolvimento de sistema que garanta a manutenibilidade, instalação e utilização. A metodologia deve contemplar, pelo menos, os seguintes aspectos:

5.1.1 Identificação dos recursos internos e externos;

5.1.2 Relacionamento com o usuário final para entendimento dos requisitos funcionais e do ambiente;

5.1.3 Definição do banco de dados (incluindo modelo de dados) e da linguagem de desenvolvimento;

5.1.4 Meios para definição dos ambientes, das estruturas de dados, das interfaces entre sistemas;

5.1.5 Formatação e procedimento para documentação das estruturas de dados, codificação, módulos e programas;

5.1.6 Critérios para codificação das rotinas;

5.1.7 Procedimento de testes;

5.1.8 Homologação: revisão dos procedimentos, preparação do ambiente, simulação e aprovação do sistema;

5.1.9 Treinamento;

5.1.10 Pós-Implantação: Avaliação de resultados e encerramento;

5.2 Todos os sistemas devem possuir documentação que deve ser armazenada em local seguro e controlado;

5.3 Todos os sistemas devem possuir trilhas de auditoria nas transações efetuadas pelos usuários e nos acessos aos códigos-fonte;

5.4 Toda autenticação deve ser feita utilizando criptografia;

5.5 O controle de acesso a todos os sistemas deve ser utilizado identificação de uso pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;

5.6 Não deve ser permitido o acesso de usuários ao banco de dados;

5.7 Os sistemas devem possuir controles para que usuários detenham acesso apenas aos recursos necessários e imprescindíveis ao desenvolvimento do seu trabalho;

5.8 Deve ser aplicado em todos os sistemas segregação de ambientes de desenvolvimento, teste, homologação, produção;

5.9 Não deve ser utilizado editores de código fonte no ambiente de produção;

5.10 Deve existir para equipe de suporte, usuários e senhas distintas e específicas para cada ambiente;

5.11 É proibido alterações no ambiente de produção sem a utilização de novos pacotes de arquivos;

5.12 Não deve ser permitido o acesso a base de dados, utilizando sempre uma aplicação e/ou sistema para realizar qualquer tipo de transação no banco de dados;

5.13 Se for necessário realizar alguma mudança em um sistema em produção deve-se garantir que o ambiente onde estão localizados os sistemas e aplicativos seja preservado, impossibilitando que seu bom funcionamento seja afetado;

5.14 Toda e qualquer solicitação de alteração nos sistemas em produção devem ser feitas somente sobe autorização do Gestor da Secretaria de Tecnologia e Informática;

5.15 Todos os sistemas devem estar em conformidade com a lei Nº 12.527/2011 para que possam atender todos os requisitos necessários para garantir o acesso a informações.

5.16 Para toda mudança nos sistemas implementada, os respectivos procedimentos de documentação devem ser atualizados;

6. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.

ANEXO IV
Norma de segurança do Ambiente Lógico

1. Apresentação

Esta Norma define a política sobre o acesso ao ambiente lógico no Ministério Público do Ceará e estabelece as diretrizes básicas a serem seguidas pelos usuários e administradores, com vistas a assegurar a prioridade de sua destinação às finalidades institucionais do Ministério Público do Ceará.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de segurança ao ambiente lógico no âmbito do Ministério Público do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança Institucional do Ministério Público do Ceará e Política de Segurança da Informação e Comunicações do Ministério Público do Ceará.

4. Definições

I - Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];

II - Software – Programa de Computador;

III - Ambiente lógico - Todo o ativo de informações das entidades;

IV - Ativo de Informação – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades;

V - Ativo de Processamento – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos;

VI - Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

VII - Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

VIII - Direito de Acesso – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

IX - Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PS da Informação das entidades;

X - Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo do Ministério Público do Ceará;

XI - Política de Segurança – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

XII - Proteção dos Ativos – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

XIII - Responsabilidade – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

XIV - Senha Fraca ou Óbvia – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

XV - Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

XVI - Proprietário do ativo – Identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo. [ISO/IEC 13335-1:2004 Item 7.1.2] ;

XVII - Custodiante do ativo – Identifica uma pessoa ou organismo que cuida do ativo no dia-a-dia [ISO/IEC 13335-1:2004 Item 7.1.2];

XVIII - Usuários – Funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários;

5. Diretrizes Gerais.

5.1 Para obter uma conta de sistema a chefia imediata deverá solicitar à Secretaria de Tecnologia e Informática, por meio de memorando assinado ou mensagem eletrônica do gestor da área, informando: nome completo do usuário, setor/órgão de lotação, matrícula e justificativa da necessidade da conta de sistema;

5.2 A Secretaria de Tecnologia e Informática efetuará o procedimento e informará ao interessado a sua credencial e Normas de uso da Internet;

5.3 A credencial deve ser confidencial e não compartilhada. O gestor imediato será responsável pelas contas de acesso à Internet pertencentes ao seu setor;

5.4 O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário;

5.5 A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só devem ser utilizado à partir de autorização formal e mediante supervisão;

5.6 A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados;

5.7 Devem ser definidos relatórios de segurança (logs) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os logs devem ser analisados periodicamente e o período de análise estabelecido deve ser o menor possível;

5.8 O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança;

5.9 Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

5.10 Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada;

5.11 Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado;

5.13 Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) devem ser utilizados para proteger as transações entre redes externas e a rede interna do Ministério Público do Ceará.

5.14 Os registros de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados;

5.15 Deve ser adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos;

5.16 Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle;

5.17 Ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão;

6 Gestão de Ativos

6.1 Os ativos tecnológicos (rede, sistemas, softwares, serviços de Internet, Correio Eletrônico, entre outros) são de propriedade do Ministério Público do Ceará e deverão ser utilizados para realização do trabalho e interesses do Ministério Público do Ceará e serão administrados e monitorados pela TI do Ministério Público do Ceará;

6.2 As informações criadas, utilizadas e armazenadas nos equipamentos do Ministério Público do Ceará são de propriedade do Ministério Público do Ceará e podem, quando necessário, serem acessadas pela Secretaria de Tecnologia e Informática, sendo, no entanto, preservada a sua integridade e confidencialidade;

6.3 Equipamentos, tráfego de rede, softwares e sistemas podem ser auditados com objetivo de manutenção e segurança;

6.4 Todos os ativos devem ser identificados e documentados a sua importância;

6.5 Todos os ativos devem possuir um responsável (proprietário), formalmente designado, que fará a correta classificação e acompanhamento periódico dos ativos;

6.6 O inventário dos ativos deve conter as informações que ajudem a assegurar a sua proteção efetiva: nome do ativo, proprietário, custodiante, localização, cópia de segurança, criticidade, dentre outros específicos;

6.7 Não será concedido o direito de administrador para os usuários de computador;

6.8 A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade;

6.9 Os dados, as informações e os sistemas de informação das entidades e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens;

6.10 As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria. Os registros devem ser protegidos e armazenados de acordo com a sua classificação;

6.11 Os sistemas e recursos que suportam funções críticas para operação das entidades, devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência;

6.12 O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, deve estar registrado e mantido atualizado em intervalos de tempo definidos pelo Ministério Público do Ceará;

6.13 O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

6.14 Os acessos lógicos devem ser registrados em logs, que devem ser analisados periodicamente. O tempo de retenção dos arquivos de logs e as medidas de proteção associadas devem estar precisamente definidos.

6.15 Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do servidor;

6.16 Os eventos devem ser armazenados em relatórios de segurança (logs) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros;

6.17 As máquinas devem estar sincronizadas para permitir o rastreamento de eventos;

6.18 Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não autorizado às informações;

6.19 A versão do Sistema Operacional, assim como outros softwares básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes;

6.20 Devem ser utilizados somente softwares autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos;

6.21 O acesso remoto a máquinas servidoras deve ser realizado adotando os mecanismos de segurança prédefinidos para evitar ameaças à integridade e sigilo do serviço;

6.22 Os procedimentos de cópia de segurança (backup) e de recuperação (restore) devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações;

6.23 Usuários e aplicações que necessitem ter acesso a recursos das entidades do Ministério Público do

Ceará devem ser identificados e autenticados;

6.24 O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha;

6.25 Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário;

6.26 A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas;

6.27 O arquivo de senhas deve ser criptografado e ter o acesso controlado;

6.28 As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);

6.29 As estações de trabalho, incluindo equipamentos portáteis ou *stand alone*, e informações devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

6.30 Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes);

6.31 Devem ser adotadas medidas de segurança lógica referentes a combate a vírus, backup, controle de acesso e uso de software não autorizado;

6.32 As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de backup, definidos em documento específico;

6.33 Os usuários devem utilizar apenas softwares licenciados pelo fabricante nos equipamentos das entidades, observadas as normas do Ministério Público do Ceará e legislação de software;

6.34 A entidade deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados;

6.35 A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado;

6.36 O inventário dos recursos deve ser mantido atualizado;

6.37 As mídias devem ser eliminadas de forma segura, quando não forem mais necessárias;

6.38 Procedimentos formais para a eliminação segura das mídias devem ser definidos, para minimizar os riscos;

6.39 Os procedimentos de combate a processos destrutivos (vírus, cavalodetróia e worms) devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores stand alone;

6.40 A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação;

6.41 Serviços vulneráveis devem receber nível de proteção adicional;

6.42 O usuário não deverá:

6.42.1 Executar atividades que sejam ilegais, classificadas como crime ou contravenção, perante as leis locais, estaduais, federais ou internacionais enquanto utilizando os recursos computacionais sob o domínio do Ministério Público do Ceará;

6.42.2 Copiar materiais protegidos por direito de cópia como digitalização e distribuição de fotografias e revistas, livros ou outras origens;

6.42.3 Utilizar os recursos computacionais do Ministério Público do Ceará para obter ou transmitir materiais políticos, pornográficos, de pedofilia, ofensivos, segregatórios, discriminatórios e que violem leis de trabalho e raciais, entre outros;

6.42.4 Promover ou manter um negócio pessoal ou privado com oferta de produtos e/ou serviços, utilizando-se dos recursos computacionais e informações do Ministério Público do Ceará, como base de operação e/ou de divulgação para ganhos pessoais;

6.42.4 Criar ou autorizar pontos de acesso;

6.42.5 Gerar interrupções na segurança da rede de comunicação;

6.42.6 Alterar o horário da estação;

6.42.7 Utilizar técnicas de obtenção de dados os quais os usuários estejam expressamente autorizados a acessar;

6.42.8 Realizar varredura na rede (port-scan ou sniffing), parada de serviços (DoS), roteamento falsificado e outros como inundação de pacotes (pinged floods), ou falsificação/ injeção de pacotes (packet spoofing) para propósitos maliciosos, a menos que estas obrigações estejam dentro do escopo de obrigações regulares;

6.42.9 Realizar varredura (busca) de portas (estrutura lógica que permite a comunicação entre computadores clientes e serviços oferecidos por computadores servidores);

6.42.10 Executar qualquer forma de monitoramento da rede que intercepte dados de usuários, a menos que esta atividade seja parte das obrigações ou função do usuário;

6.42.11 Executar atividades com intenção de enganar a autenticação do usuário ou segurança de qualquer serviço, computador, rede ou conta de qualquer organização, incluindo o uso de ferramentas de hardware ou software para remover/burlar a proteção de cópias de software, descobrir senhas, identificar vulnerabilidades de segurança, decodificar arquivos codificados, ou comprometer a segurança da informação por qualquer outro modo;

6.42.11 Executar quaisquer processos que envolvam suporte técnico, tais como abrir computadores ou mudá-los de localização, alteração nas configurações, instalação e desinstalação de recursos computacionais, exceto para usuários que têm essa atividade como função;

6.42.12 Utilizar programas/scripts/comandos, ou envio de mensagens de qualquer tipo, com a intenção de interferir ou desabilitar uma sessão autenticada de um usuário, através de qualquer meio, localmente ou via rede;

6.42.13 Apropriação ou cópia de arquivos eletrônicos sem permissão;

6.42.14 Visualização de arquivos e contas de outras pessoas, exceto no caso de tais atividades estarem dentro das obrigações da sua função;

6.42.15 Executar atividades não oficiais, tais como jogos eletrônicos, chats (bate- papo), programs P2P e Instant Messenger;

6.42.16 Escrever, copiar, executar, ou tentar introduzir qualquer código computacional designado para se auto-replicar, danificar, ou atrasar a performance de acesso para qualquer computador corporativo, rede ou informação;

6.42.17 Acessar outras redes usando modem ou outros mecanismos de acesso remoto sem a aprovação da Secretaria de Tecnologia e Informática;

6.42.18 Trazer descrédito para o Ministério Público do Ceará, seus parceiros e colaboradores;

6.42.19 Revelar, sem autorização, qualquer informação do Ministério Público do Ceará que não seja pública;

6.42.20 Desativar, em hipótese alguma, o software de detecção e reparo de software/código malicioso;

6.43 CONTAS E SENHAS PARA USUÁRIOS

6.43.1 Toda conta de usuário precisa possuir senha e deve seguir os padrões estabelecidos nesta Norma;

6.43.2 Todas as senhas de usuários de acesso a rede, sistemas e serviços diversos do Ministério Público do Ceará deverão ser trocadas a cada 30 dias;

6.43.3 As contas de rede serão bloqueadas depois de 5 (cinco) tentativas inválidas de entrada. Para destravar o usuário deverá entrar em contato com a Secretaria de Tecnologia e Informática;

6.43.4 Na criação de uma nova conta, o usuário receberá uma senha temporária, a qual deverá ser trocada no primeiro acesso;

6.43.5 As contas que ficarem inativas por mais de 90 (noventa) dias corridos serão bloqueadas;

6.43.6 A senha deverá conter no mínimo 6 (seis) caracteres;

6.43.7 A senha deve ser definida com letras, números, e caracter especial tipo: #, @, $,%, &, !, *, ?, _,/, <>,:,;, {}, [], =, +

6.44 Deveres do Usuário

6.44.1 Trocar a senha temporária no primeiro acesso;

6.44.2 Não registrar a senha em papel, em local visível, no computador ou na Internet;

6.44.3 Nunca utilizar o recurso de "Relembrar a senha" ou semelhantes de aplicações como navegadores, correio eletrônico, entre outras;

6.44.4 Trocar a senha quando houver suspeita de haver sido comprometida e comunicar o incidente ao setor de TI;

6.44.5 Não revelar senhas pelo telefone, e-mail ou por qualquer outro meio para NINGUÉM, mesmo que seja o chefe, assistentes ou secretárias;

6.44.6 Não revelar senhas em questionários ou formulários;

6.44.7 Não permitir que alguém observe você digitando sua senha;

6.44.8 Não revelar senhas para colegas de trabalho enquanto estiver de férias ou licença;

6.45 Responsabilidades do Usuário

6.45.1 O usuário é o responsável pelos acessos aos serviços realizados pela sua conta;

6.45.2 O mau uso de uma conta de acesso aos serviços por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;

6.45.3 Zelar pelo fiel cumprimento ao estabelecido nesta Norma;

6.46 CONTAS E SENHAS PARA ADMINISTRADORES

6.46.1 Toda conta com privilégio de administrador precisa possuir senha e deve seguir os padrões estabelecidos nesta Norma;

6.46.2 A senha deverá conter no mínimo 10 (dez) caracteres. No caso dos ambientes que não suportarem o mínimo de 10 caracteres, deverão ser utilizados o limite máximo que o ambiente permitir;

6.46.3 Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação de mínimo de 10 caracteres ou conforme o ambiente;

6.46.4 As contas com privilégio de administrador não poderão conter em sua formação algo que as identifique como sendo uma conta de administrador. (Ex: Admin, Adm, Administrador, Administrator, pradmin etc.);

6.46.5 As senhas devem possuir números, letras minusculas e maiúsculas e caracteres especiais;

6.46.6 A conta deverá ser bloqueada após a 5ª (quinta) tentativa inválida de entrada;

6.46.7 O tempo de vida das senhas deverá obedecer aos seguintes critérios:

6.46.8 No caso de suspeita do comprometimento de uma senha, esta deverá ser reinicializada;

6.46.9 Se algum usuário souber sobre qualquer violação a esta Norma deverá comunicar a Secretaria de Tecnologia e Informática ou a sua chefia imediata;

6.47 Responsabilidades da Secretaria de Tecnologia e Informática

6.47.1 Criar e manter as contas de sistemas e serviços;

6.47.2 Adotar mecanismos para bloquear a senha após 5 (cinco) tentativas inválidas;

6.47.3 Adotar mecanismos para não aceitar senha com menos de 6 (seis) caracteres;

6.47.4 Adotar mecanismos para forçar o usuário a trocar a senha no primeiro acesso;

6.47.5 Instruir os usuários na criação de senhas e a sua importância na segurança da informação;

6.47.6 Adotar mecanismos de periodicamente enviar para as chefias imediatas, uma relação das contas em quais serviços que estão sob sua responsabilidade;

6.47.7 As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada;

6.47.8 Sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias;

6.47.9 As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas;

6.47.10 A distribuição de senhas aos usuários (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário, no primeiro acesso;

6.47.11 O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só deve ser executada após a identificação positiva do usuário. A senha digitada não deve ser exibida;

6.47.12 Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas;

6.47.13 O sistema de controle de acesso deve exibir, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão, o sistema deve exibir para o usuário informações sobre o último acesso;

6.47.14 Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso;

6.48 Responsabilidades da Diretoria de Recursos Humanos

6.48.1 O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos do Ministério Público do Ceará;

6.48.2 Será necessário que o setor de Recursos Humanos relacione claramente as atribuições de cada função do novo empregado, de acordo com a característica das atividades desenvolvidas, a fim de determinar o perfil necessário do empregado ou servidor, considerando os seguintes itens:

a) a descrição sumária das tarefas inerentes à função;
b) as necessidades de acesso a informações sensíveis;
c) o grau de sensibilidade do setor onde a função é exercida;
d) as necessidades de contato de serviço interno e/ou externo;
e) as características de responsabilidade, decisão e iniciativa inerentes à função;
f) a qualificação técnica necessária ao desempenho da função.

6.48.3 Deve ser definido um processo pelo qual será apresentada aos empregados,

servidores e prestadores de serviço esta Política de Segurança e as normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento;

6.48.4 O acesso de exservidores ou colaboradores às instalações, quando necessário, será restrito às áreas de acesso público;

6.48.5 Quando o empregado for desligado do Ministério Público do Ceará deverá ser retirada sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados;

6.48.6 O empregado ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a entidade, devendose checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações;

6.48.7 Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades;

7. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.

ANEXO V
Norma de segurança do Ambiente Físico

1. Apresentação

Esta Norma define a política sobre o acesso ao ambiente físico no Ministério Público do Ceará e estabelece as diretrizes básicas a serem seguidas pelos usuários e administradores, com vistas a assegurar a prioridade de sua destinação às finalidades institucionais.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de segurança ao ambiente físico no âmbito do Ministério Público do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança Institucional do Ministério Público do Ceará e Política de Segurança da Informação e Comunicações do Ministério Público do Ceará.

4. Definições

I - Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];

II - Software – Programa de Computador;

III - Ambiente lógico - Todo o ativo de informações das entidades;

IV - Ativo de Informação – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das entidades;

V - Ativo de Processamento – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos;

VI - Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

VII - Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

VIII - Direito de Acesso – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

IX - Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades;

X - Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da PGJ;

XI - Proteção dos Ativos – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

XII - Responsabilidade – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

XIII - Senha Fraca ou Óbvia – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

XIV – Servidor – Máquia destinada a fornecer determinado serviço ou recurso para as estações da rede do Ministério Público;

5. Diretrizes Gerais.

5.1 As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização;

5.2 Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos servidores;

5.3 Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida;

5.4 Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas ao responsável pela gerência de segurança da entidade. Ele deverá tomar as medidas apropriadas para prevenir acessos não autorizados;

5.5 Os servidores deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência;

5.6 Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados;

5.7 A entrada e saída, nestas áreas ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência da Secretaria de Tecnologia e Informática e mantidas em local adequado e sob sigilo;

5.8 O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, deverá ser restrito ao pessoal autorizado;

5.9 O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente;

5.10 Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só devem ser utilizados a partir de autorização formal e mediante supervisão;

5.11 Nas instalações da PGJ, todos deverão utilizar alguma forma visível de identificação (por exemplo: crachá), e devem informar à segurança sobre a presença de qualquer pessoa não identificada ou

de qualquer estranho não acompanhado;

5.12 Visitantes das áreas de segurança devem ser supervisionados. Suas horas de entrada e saída e o local de destino devem ser registrados. Essas pessoas devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada;

5.13 Os ambientes onde ocorrem os processos críticos das entidades integrantes da PGJ deverão ser monitorados, em tempo real, com as imagens registradas por meio de sistemas de Circuito Fechado de Televisão CFTV;

5.14 Sistemas de detecção de intrusos devem ser instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado;

6. Penalidades

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente e no Regimento Interno de Pessoal ou em qualquer outra legislação que regule ou venha regular a matéria.