



**MINISTÉRIO PÚBLICO DO ESTADO DO CEARÁ
PROCURADORIA GERAL DA JUSTIÇA**

PROVIMENTO nº 119/2010/PGJ

Institui a Política de Segurança Institucional e o Plano de Segurança Institucional e dá outras providências.

A PROCURADORA-GERAL DE JUSTIÇA, no uso das atribuições previstas no art. 26, XVIII, da Lei Complementar Estadual n. 72, DE 16 de dezembro de 2008 – Lei Orgânica e Estatuto do Ministério Público do Estado do Ceará,

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

CONSIDERANDO a necessidade de se criarem normas de proteção e segurança institucional, orgânica e ativa;

CONSIDERANDO que a salvaguarda de assuntos sigilosos traduz-se na preservação e manutenção da sua confiabilidade, integridade e disponibilidade;

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 contato com estes;

CONSIDERANDO a necessidade da consolidação da política de segurança e a criação do Plano de Segurança Institucional;

CONSIDERANDO a criação do Núcleo de Inteligência e Segurança Institucional do Ministério Público, instituído por meio do Provimento n. 95, de 01 de outubro de 2010, publicado no DJE de 19 de outubro de 2010 com a finalidade de produzir conhecimento para a tomada de decisões estratégicas, dentre outras premissas regentes; e

CONSIDERANDO a Recomendação n. 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,

RESOLVE:

Art. 1º Fica criada e instituída a Política de Segurança Institucional, conforme Anexo Único.

Art. 2º Fica criado e instituído o Plano de Segurança Institucional (PSI).

Art. 3º O Procurador-Geral de Justiça editará atos necessários para a operacionalização das diretrizes, ações e normas contidas na Política de Segurança Institucional e no Plano de Segurança Institucional.

Art. 4º A difusão da Política de Segurança Institucional e a execução do Plano de Segurança Institucional (PSI) do Ministério Público do Estado do Ceará, serão realizadas gradativamente, observadas as condições orçamentárias.

Art. 5º Compete à Coordenadoria do Núcleo de Inteligência e Segurança Institucional editar, exclusiva ou conjuntamente com outros órgãos, Plano de Atuação (PA) para detalhamento das ações de execução da Política de Segurança Institucional e do Plano de Segurança Institucional (PSI).

Art. 6º A Política de Segurança Institucional, contida no Anexo Único, deverá ser difundida no âmbito do Ministério Público do Ceará.

Art. 7º Por medida de segurança, estrategicamente, o Plano de Segurança Institucional 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, no prazo de 30 (trinta) dias.

Art. 8º As disposições, os princípios e as diretrizes previstas na Política de Segurança Institucional, além das normas, ações e providências preconizadas no Plano de Segurança Institucional, possuem natureza obrigatória, de modo que o seu descumprimento poderá acarretar sanções previstas no ordenamento jurídico pátrio.

Art. 9º Este Provimento entra em vigor na data de sua publicação.

PUBLIQUE-SE, REGISTRE-SE E COMUNIQUE-SE.

GABINETE DA PROCURADORA-GERAL DE JUSTIÇA, em Fortaleza, aos 06 de dezembro de 2010.


MARIA DO PERPÉTUO SOCORRO FRANÇA PINTO
PROCURADORA-GERAL DE JUSTIÇA

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA INSTITUCIONAL e PLANO DE SEGURANÇA INSTITUCIONAL

CONTEXTUALIZAÇÃO

A elaboração de uma **Política de Segurança Institucional** e de um **Plano de Segurança Institucional** nasce da premissa, dos dias modernos, da necessária proteção que os entes públicos devem dar ao seus **integrantes**, bem como ao seu **patrimônio**, e ainda para tornar seguro todo o **conhecimento produzido** em suas áreas de atuação, evitando assim o **comprometimento** de tal **patrimônio** e **conhecimentos**, que estão voltados para cumprir a missão constitucional estabelecida nos arts. 129 e seguintes da Constituição Federal.

Para alcançar os objetivos definidos nas Constituições Federal e Estadual, o **Ministério Público do Estado do Ceará** deve ser munido de instrumentos capazes de fazer frente às constantes **ameaças** e **vulnerabilidades** em relação aos seus **integrantes**, **patrimônio** e **conhecimentos**, isto em um **plano contínuo**.

O tema Segurança Institucional surge nos tempos modernos como uma forma de prevenção contra a criminalidade e a violência voltadas contra as instituições públicas que tem como objetivo a garantia do efetivo respeito à ordem constitucional e às leis.

I. POLÍTICA DE SEGURANÇA INSTITUCIONAL

a) OBJETIVO

O objetivo da **Política de Segurança Institucional do Ministério Público do Estado do Ceará** é a de criar condições para a implantação de normas e procedimentos para a aplicação de um **Plano de Segurança Institucional**, que tem por objetivo geral a **integridade** de seu **patrimônio**, quer material ou humano, assegurando a contínua defesa da Constituição Federal e colaborar com a continuidade do **interesse institucional** e do dever constitucional.

A adoção da **Política de Segurança Institucional** no âmbito do **Ministério Público do Estado do Ceará** e do **Plano de Segurança Institucional** é dever de todos os **integrantes** da instituição e visam a manutenção de seus **serviços essenciais** .

b) INTRODUÇÃO

A **Política de Segurança Institucional** do Ministério Público do Estado do Ceará é derivada da Recomendação nº 13 do Conselho Nacional do Ministério Público e do Provimento nº 71/2008 de 18/08/2008 da Procuradoria Geral de Justiça do Estado do Ceará.

A adoção de uma **Política de Segurança Institucional**, além das exigências legais de preservação do patrimônio público e do Ministério Público, visa abranger as áreas definidas pela Recomendação nº 13 do Conselho Nacional do Ministério Público e que são: Áreas e Instalações, Informática e Comunicações, Pessoal, Documentos e Material.

A **Política de Segurança Institucional do Ministério Público** e o **Plano de Segurança Institucional**, serão conduzidos e implantados no **Programa Permanente de Segurança Institucional (PPSI)**.

O **Programa Permanente de Segurança Institucional (PPSI)** deverá abranger como metas as seguintes áreas, para as quais serão criados subgrupos com as seguintes designações :

- Subgrupo **Áreas e Instalações;**
- Subgrupo **Informática e Comunicações ;**
- Subgrupo **Pessoal;**
- Subgrupo **Materiais e Documentos.**

Cada subgrupo será coordenado pelo Diretor da área específica acima indicada ou por nomeação do(a) Procurador(a) Geral de Justiça.

Cabe ao Coordenador de cada Subgrupo, juntamente com o Coordenador do **Programa Permanente de Segurança Institucional (PPSI)**, elaborar o **plano de atuação** de sua área, dentro das diretrizes do **Plano de Segurança Institucional** abaixo descritas, submetendo-o a(o) Procurador(a) Geral de Justiça, para a devida implantação.

Para consecução dos objetivos da **Política de Segurança Institucional**, o **Ministério Público do Estado do Ceará** e suas unidades podem recorrer aos órgãos governamentais de segurança pública ou de atendimento de emergência.

Esta política deve ser seguida quando do relacionamento do Ministério Público do Estado do Ceará com outras Instituições governamentais ou não, nacionais ou estrangeiras.

Nessas situações serão desenvolvidas negociações que demarquem as responsabilidades na área de segurança e a obediência aos acordos mantidos entre as partes.

O compartilhamento e classificação de informações e tecnologias da informação, atividades *online* e outros propósitos, devem ser adequado às exigências de segurança estabelecidas nesta política.

As exigências desta política complementam outras medidas do **Ministério Público do Estado do Ceará**, no enfrentamento de situações de emergência (incêndios, ameaças de bomba, materiais perigosos, falta de energia, evacuação, emergências civis, etc).

C) ATUAÇÃO ESPECÍFICA

D) Áreas e Instalações

No item áreas e instalações a atuação deve estar voltada para prevenção de acessos não autorizados e respostas efetivas e imediatas contra tais atos, devendo suas **instalações** serem projetadas ou reformadas para que tal objetivo seja alcançado.

Constitui ainda função desta **Política de Segurança Institucional** dotar o **Ministério Público do Estado do Ceará** de salvaguardas para proteção de suas **instalações** contra atos de vandalismo, incêndios e outros que necessitem de uma melhor atenção na busca da efetiva segurança.

II) Informática e Comunicações

A **Política de Segurança Institucional** no item **Informática e Comunicações** terá como item base a **segurança da informação**, sua **integridade** e **disponibilidade**, assegurando aos membros do **Ministério Público do Estado do Ceará** a utilização segura para o desempenho das funções constitucionais, bem como para evitar o seu **comprometimento**.

III) Pessoal

A **Política de Segurança Institucional** no item pessoal visa dotar o **Ministério Público do Estado do Ceará** de medidas de gerenciamento dos recursos humanos, quer na contratação de servidores, efetivos ou não, membros ou terceirizados, e que todos estejam voltados para o efetivo exercício de sua missão constitucional, bem como a salvaguarda de caráter pessoal de todos, e ainda de dotá-los de uma conscientização de métodos e procedimentos para o trato com assuntos que devem guardar sigilo.

IV) Materiais e Documentos

A **Política de Segurança Institucional** no item materiais e documentos tem a função de dotar o **Ministério Público do Estado do Ceará** de medidas de segurança para o resguardo e manuseio de materiais e documentos.

Tem ainda como função primordial o estabelecimento de procedimentos para arquivamento de documentos, seu descarte, bem como dos materiais.

II. PLANO DE SEGURANÇA INSTITUCIONAL

(a) CONSIDERAÇÕES

São metas do **Plano de Segurança Institucional**: dotar o **Ministério Público do Estado do Ceará** de um ordenamento e de uma consciência voltada à segurança de seus membros, do seu patrimônio e da proteção do conhecimento obtido nas diversas áreas nas quais atua e cujas funções são ordenadas na Constituição Federal

Com a função constitucional dada ao **Ministério Público** pela Constituição Federal e demais leis, bem como a sua função ativa contra diversos interesses, é evidente que o **Ministério Público do Estado do Ceará**, sofre e poderá sofrer constantemente ações danosas contra seu patrimônio, físico, lógico ou humano, nos quais se incluem atentados, acessos não autorizados, subtração ou destruição de bens e informações, além de outros.

Com o crescente desenvolvimento tecnológico posto à disposição dos membros do **Ministério Público do Estado do Ceará**, bem como as atividades ilegais na área de **informática**, os **cibercrimes** e outras atividades danosas que podem causar vários prejuízos à instituição, e aos

seus membros, o **Plano de Segurança Institucional** está voltado para impedir que tais fatos ocorram ou para minimizar seus danos.

Este **Plano de Segurança Institucional** deve ser obedecido por todos os integrantes do **Ministério Público do Estado do Ceará**.

O presente plano se complementa pelas normas e planos executivos existentes ou a serem elaborados em obediência à **Política de Segurança Institucional**.

As **Unidades** e os **integrantes** do Ministério Público deverão cumprir as exigências deste **Plano de Segurança Institucional** e da **Política de Segurança Institucional**, suas normas, planos executivos e documentação técnica associada.

As exigências são baseadas na análise integrada e contínua das **avaliações de riscos e ameaças** contra o Ministério Público realizadas pelos órgãos responsáveis pela Segurança Institucional (**Programa Permanente de Segurança Institucional (PPSI)**).

As Unidades do **Ministério Público do Estado do Ceará**, poderão conduzir suas próprias avaliações de ameaças e riscos, ou solicitar que sejam realizadas por servidor qualificado, para determinar as suas necessidades de proteção, repassando-as ao **Programa Permanente de Segurança Institucional (PPSI)** responsável pela Segurança Institucional para análise e providências cabíveis.

O **Programa Permanente de Segurança Institucional (PPSI)** responsável pela Segurança Institucional orientará as Unidades na implementação de níveis mais elevados de segurança em situações de emergência.

Para melhor aplicação do Plano de Segurança Institucional, serão utilizados os seguintes termos:

Ameaça - Qualquer evento ou ato, deliberado ou não e intencional, que possa causar dano a membros do Ministério Público do Estado do Ceará ou a sua estrutura física ou lógica.

Áreas ocupadas - Todo espaço físico em utilização pelo Ministério Público do Estado do Ceará cujas instalações estão sob a administração de outros entes públicos.

Áreas integrantes - Todo espaço físico em utilização pelo Ministério Público do Estado do Ceará cujas instalações estão sob sua administração.

Área Controlada – Conjunto de áreas onde, apesar de composição com outras áreas de acesso aberto podem ter o acesso limitado a pessoas autorizadas.

Área de acesso restrito – Área de trabalho onde o acesso é limitado a pessoas autorizadas.

Autenticidade: asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino.

Autorização -. Autorização oficial de pessoa habilitada para que outra tenha acesso a sistemas de tecnologia de informação.

Bens Essenciais – Bens que dão suporte a serviços essenciais do Ministério Público do Estado do Ceará.

Bens Protegidos – Bens cuja revelação não autorizada se possa esperar dano a interesses institucionais.

Classificação: atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação.

Comprometimento – perda de segurança resultante do acesso não-autorizado - Revelação não autorizada, destruição, remoção, modificação, interrupção ou uso de bens do Ministério Público do Estado do Ceará.

Confidencialidade – O atributo conferido a uma informação ou documento que impede o acesso ou a sua revelação a pessoas não autorizadas.

Credencial de Acesso Credencial exigida para o acesso a instalações essenciais ao interesse do Ministério Público do Estado do Ceará.

Desclassificação: cancelamento, pela autoridade competente ou pelo transcurso de prazo, da classificação de documentos ou de acesso a intranet ou a banco de dados;

Disponibilidade: facilidade de recuperação ou acessibilidade de dados e informações;

Documentos classificados – É a confidencialidade atribuída a um documento ou a grupos de documentos.

Exigências básicas de Segurança – Diretrizes mínimas adotadas como padrão operacional na Política e no Plano de Segurança institucional.

Grau de sigilo: gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

Incidente de Segurança – Qualquer ação ou omissão voltada para o comprometimento de bens, pessoais, físicos ou lógicos do Ministério Público do Estado do Ceará ou contra seus membros e servidores em efetivo serviço ou decorrente deles.

Informação classificada – Informação dotada de interesses institucional do Ministério Público e que recebeu a classificação devida.

Instalações – Ambiente físico destinado ao uso de integrantes do Ministério Público do Estado do Ceará. Uma instalação pode ser parte de um prédio, um prédio inteiro ou um prédio e sua área; ou pode ser uma construção em que não existe edificação. O termo abrange não apenas o objeto mas também o seu uso.

Integrantes - Procuradores de Justiça, Promotores de Justiça, Servidores (concursados ou não).

Integridade – Precisão e incolumidade de bens e dados e a autenticidade das transações na origem, no trânsito ou no destino.

Interesse Institucional – Interesse referente à defesa e manutenção dos objetivos institucionais do Ministério Público do Estado do Ceará.

Motivo Determinante – Uma determinação da existência de razões suficientes para rever, revogar, suspender ou diminuir o status de confiabilidade ou de uma medida de proteção.

Necessidade de conhecer A necessidade que alguém possui de acessar e conhecer informações necessárias ao cumprimento de seu dever.

Patrimônio – Coisas tangíveis ou intangíveis pertencentes ao Ministério Público do Estado do Ceará, informações em todas as suas formas e mídias, redes, sistemas, bens, recursos financeiros.

Plano Contínuo – Um conjunto de atos que incluem o desenvolvimento e a pontual execução de planos, medidas, procedimentos e arranjos que garantam a disponibilidade mínima ou a não interrupção da disponibilidade de serviços e bens essenciais a atividade do Ministério Público do Estado do Ceará .

Segurança das Comunicações -. Criptografia, transmissão e emissão de medidas de segurança aplicadas ao arquivamento, processamento ou transmissão eletrônica; um subconjunto da segurança de tecnologia de informações.

Segurança de Tecnologia de Informação –. Salvaguardas para preservar o sigilo, integridade, disponibilidade, uso e valor de informações eletronicamente arquivadas.

Segurança Física - (segurança material) – O uso de salvaguardas físicas para prevenir e retardar o acesso não autorizado a bens, detecção antecipada e ativar resposta apropriada.

Sistema de Informática – *Todo o conjunto de computadores, programas à disposição do Ministério Público do Estado do Ceará, em rede ou não*

Serviços Essenciais – Serviços cujo comprometimento em termos de disponibilidade ou integridade poderão resultar em alto grau de dano à saúde, proteção e ao patrimônio dos usuários dos serviços e ao eficiente funcionamento do Ministério Público do Estado do Ceará .

Visita- pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa.

Visitante - pessoa cuja entrada foi admitida a acessar qualquer área, com exceção das áreas sigilosas.

Vulnerabilidade Falha na segurança que pode permitir que a transformação de uma ameaça em dano.

(b) ÁREAS ENVOLVIDAS

Este **Plano de Segurança Institucional** abrange as áreas indicadas na **Política de Segurança Institucional** e são:

- Áreas e Instalações;
- Informática e Comunicações;
- Pessoal;
- Documentos e Material.

(c) EXECUÇÃO

Para a execução deste **Plano de Segurança Institucional** serão designadas os **subgrupos** definidos na **Política de Segurança Institucional**, para que sejam aplicadas as diretrizes abaixo e que devem ser obedecidas por todos os **integrantes** do **Ministério Público do Estado do Ceará**.

(d) DIRETRIZES PARA EXECUÇÃO DO PLANO DE SEGURANÇA INSTITUCIONAL

D.1 . ÁREAS e INSTALAÇÕES

D.1.1 Divisão de áreas

1.1.1- As **instalações** do Ministério Público do Estado do Ceará, para uma efetiva proteção do seu **patrimônio e informações**, bem como para controle de acesso pelo público e, em menor extensão, por **integrantes** serão definidas da seguinte forma:

- **Áreas Públicas;**
- **Áreas de Recepção;**
- **Áreas de Operação;**
- **Áreas de Segurança;**

1.1.2- As duas primeiras destas quatro áreas (**áreas públicas e áreas de recepção**) devem estabelecer condições de acesso para as demais duas áreas, sendo que a última é considerada **área de acesso restrito**.

1.1.3- O termo **área controlada** pode ser usada para descrever qualquer combinação de **áreas de segurança**. Por exemplo: quando um conjunto de áreas de segurança são separadas por áreas de acesso público e de recepção.

1.1.4- Uma **Área pública** geralmente cerca ou forma parte de uma instalação do **Ministério Público do Estado do Ceará**. Exemplos incluem

o terreno em volta do prédio, corredor público e lobbies de elevador em prédio de ocupação mista. Indicativos de limites tais como sinais e vigilância direta ou remota devem ser usados para desencorajar atividade não autorizada.

1.1.5- A **área de recepção** deve ser localizada na entrada da instalação. É o local onde o contato inicial entre o público e o **Ministério Público do Estado do Ceará** ocorre, onde os serviços são providos, informações são trocadas e os acessos as demais áreas são controlados.

1.1.6- Com variados graus, a atividade na **área de recepção** deve ser monitorada por pessoal que ali trabalha, por outras pessoas ou pelo corpo de segurança.

1.1.7- O Acesso pelo público, por razões específicas, pode ser limitado a períodos determinados do dia.

1.1.8- O acesso além da **área de recepção** deve ser monitorado pelo corpo de segurança.

1.1.9- Uma **Área de Operação** é uma área onde o acesso é limitado ao pessoal que ali trabalha e a visitantes identificados.

1.1.10- **Áreas de operação** devem ser monitoradas e devem, preferencialmente, ser acessíveis a partir da **área de recepção**.

1.1.11- Uma **área de segurança** é uma área onde o acesso é limitado a pessoal autorizado e a visita devidamente acompanhada.

1.1.12- **Áreas de Segurança** devem preferencialmente ser acessíveis a partir da Área de Operação e através de um ponto de entrada.

1.1.13- Uma **Área de segurança** necessita ser separada de uma Área de operação por um perímetro seguro.

1.1.14- **Áreas de segurança** devem ser monitoradas 24 horas ao dia e sete dias por semana pelo corpo de segurança, outras pessoas ou por meios eletrônicos.

1.1.15- No prédio principal do **Ministério Público do Estado do Ceará**, os gabinetes dos Procuradores e Promotores de Justiça devem ser tratados como **Áreas de Operação**.

1.1.16- Uma *Área de Segurança* é uma área na qual o acesso é controlado através de um ponto de entrada e limitado a pessoas autorizadas e devidamente submetidas a procedimento de checagem de confiabilidade e a visitantes adequadamente identificados e acompanhados.

1.1.17- **As Áreas de Segurança** devem ser acessíveis apenas a partir de Áreas de Operação e separadas das demais áreas por um perímetro construído segundo especificações contidas na Avaliação de Risco e Ameaças.

D 1.2. Segurança Física

1.2.1- A **segurança física** envolve o necessário planejamento das instalações, bem como no uso de medidas específicas de segurança para prevenir o acesso não autorizado de pessoas nas instalações ou áreas ocupadas do **Ministério Público do Estado do Ceará**, bem como para prevenir e evitar *ameaças*;

1.2.2- Em todas as instalações do **Ministério Público do Estado do Ceará**, caso necessário, e a serem definidas pelo subgrupo *áreas e instalações*, serão inseridos pontos de controle de acesso com bloqueios e com a finalidade de registros das pessoas que tenham acesso ao seu interior.

1.2.3- A segurança física também deve prover medidas de segurança de integrantes, usuários, visitantes e prestadores de serviço contra ameaças e violência nas dependências das *instalações* da Instituição.

1.2.4- O sistema de **segurança física** deve estar totalmente integrado aos projetos de construções, ampliações ou reformas de instalações e seguir **exigências básicas de segurança** .

1.2.5- As **instalações** devem ser selecionadas, projetadas ou modificadas de modo a facilitar o **controle de acesso**. Durante os processos de projeção das **instalações** provavelmente serão criadas vulnerabilidades na segurança e a sua posterior reforma tornará oneroso tal projeto. Para que se evite tais situações, os responsáveis pelo **Programa Permanente de Segurança Institucional(PPSI)** deverão estar cientes dos planos de projeção das instalações e devem colaborar com os membros na elaboração do projeto para assegurar que as considerações de segurança serão levadas em conta na seleção das instalações e desenho das construções ou espaços .

1.2.6- As *áreas de acesso restrito* devem ser demarcadas e controladas por barreiras físicas e/ou sistemas eletrônicos de controle de acesso ou detecção conforme recomendado em avaliação de ameaças e riscos pelo subgrupo *áreas e instalações* e pelo **Programa Permanente de Segurança Institucional (PPSI)**.

1.2.7- Os **integrantes** do Ministério Público do Estado do Ceará que ocupem posições de alto risco pessoal devem ser protegidos contra atos de violência e outros que possam dificultar ou impedir o exercício de suas funções constitucionais .

1.2.8- As saídas de emergência devem satisfazer as preocupações com a segurança dos integrantes, mas não devem permitir acesso não autorizado a áreas restritas, tanto em situação normal quanto em emergências.

1.2.9- As medidas de segurança física das instalações obedecerão aos regulamentos e códigos federais, estaduais e municipais inerentes ao assunto. Esses regulamentos incluem Códigos de Edificações, Planos Diretores, e normas de Direito do Trabalho, de combate a incêndio, assim como regulamentos para construção e circuitos elétricos.

1.2.10- Os muros e cercas , obrigatoriamente devem delinear os limites, delimitar a propriedade, fornecer algum controle sobre o acesso, facilitar a vigilância das instalações e o controle do perímetro.

1.2.11- A segurança também deve ser considerada no projeto ambiental da paisagem em volta ou nas proximidades das instalações.

1.2.12- A paisagem deve facilitar a proteção dos edifícios, detecção de intrusos e resposta a incidentes de segurança.

1.2.13- Ao mesmo tempo, as medidas de segurança da paisagem não devem interferir com o valor estético da propriedade.

1.2.14- Medidas paisagísticas de segurança úteis incluem a definição clara dos limites, a ausência de esconderijo para intrusos e Uma visão desobstruída de áreas problemáticas.

1.2.15- Nos estacionamentos da Instituição as vagas devem estar convenientemente distantes de saídas de emergência, áreas de carga e descarga e outras aberturas e devem permitir que vigilantes e servidores monitorem veículos e pedestres;

1.2.16- A segurança das instalações e de estacionamento pode ser incrementada pelo correto encaminhamento de veículos para e do estacionamento de modo a que se tenha controle dos possíveis pontos vulneráveis.

1.2.17- O projeto de áreas de estacionamentos e suas reformas deverão conduzir os motoristas a que entrem e deixem a área pelo ponto mais remoto das instalações. Isto possibilitará as atividades de vigilância de veículos estacionados e de pedestres enquanto usuários se aproximam ou deixam as instalações.

D.1.3. Segurança fora de áreas e instalações da Instituição

1.3.1- No caso de Unidade instalada em prédios não destinados exclusivamente às atividades da Instituição(**áreas ocupadas**), deverão ser baixadas normas especiais de segurança.

1.3.2- Se o cumprimento desta política impuser restrições aos outros ocupantes do prédio, estes deverão ser consultados ou, no mínimo, informados se as restrições forem impostas por se tratar de área particularmente perigosa.

1.3.3- Para a salvaguarda de assuntos, documentos, bens ou áreas sensíveis deverão ser estabelecidas limitações e condições de acesso.

1.3.4- Os integrantes da Instituição em viagens para áreas ou execução de tarefas particularmente perigosas poderão requerer informações, medidas específicas de segurança e limitações ao **Programa Permanente de Segurança Institucional (PPSI)**, responsável pela Segurança Institucional.

D.2. INFORMÁTICA e COMUNICAÇÕES

D.2.1 Segurança da informação

2.1.2- A **segurança da Informação** tem como objetivo fomentar o uso adequado e seguro das informações produzidas ou recebidas no **Ministério Público do Estado do Ceará**, protegendo-as contra destruição, modificação ou divulgação indevida, quer sejam acidentais ou intencionais, visando ainda a melhoria contínua dos processos internos e serviços prestados à sociedade.

2.1.3- Com a **segurança da informação** o **Ministério Público do Estado do Ceará**, deve assegurar a garantia ao direito individual e coletivo das

pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição Federal.

2.1.4- **O Ministério Público do Estado do Ceará** deve implementar e manter ativos programas destinados à formação, capacitação, aprimoramento e conscientização de seus integrantes e prestadores de serviço com atribuições específicas na manutenção da **Segurança da Informação e Segurança das Comunicações** .

2.1.5- É vedado o uso de recursos de Tecnologia da Informação e de comunicações da Instituição com o propósito de constranger, assediar, ofender, caluniar ou ameaçar qualquer pessoa física ou jurídica; veicular opiniões político-partidárias; obter vantagem indevida para si ou para outrem; causar dano a patrimônio da Instituição ou de terceiros.

2.1.6 - Para a efetiva segurança do **Sistema de Informática** deverão ser criados, adquiridos ou locados, equipamentos (SOFTWARES e HARDWARES) necessários a obtenção do objetivo que é impedir ações invasivas em tais sistemas

2.1.7 - A segurança dos **sistemas de informática** tem como objetivo fomentar o uso adequado e seguro das informações, protegendo-as contra **incidentes de segurança**, destruição, modificação ou divulgação indevida, quer sejam acidentais ou intencionais, e a melhoria contínua dos processos internos e serviços prestados à sociedade, bem como garantir a **autenticidade da informação** .

2.1.8 - O acesso a intranet do **Ministério Público do Estado do Ceará** somente poderá ser efetuada por pessoa portadora de **autorização**, devidamente habilitada e registrada no setor de informática mediante login e senha de acesso que deverão ser constantemente atualizados e modificados e desabilitados quando o **integrante** for desligado da instituição.

2.1.9 - O setor de informática, através do subgrupo **Informática e Comunicações** deverão atuar ativamente na realizações de seminários, cursos, palestras e informes voltados á conscientização de todos os membros do Ministério Público do Estado do Ceará, sobe a necessidade da **Segurança da Tecnologia da Informação**.

D.3. PESSOAL

3.1.1- Este plano se aplica a todos os processos de contratação de pessoal, (concurados, comissionados ou terceirizados), empresas e convênios firmados pelo Ministério Público.

3.1.2- Deverão ser observadas as exigências deste plano e mais:

- a. Assegurar a correta avaliação de confiabilidade de organizações privadas contratadas e indivíduos que necessitem ter acesso a informações e a **bens protegidos** e classificados como sigilosos;
- b. Assegurar a proteção de **bens essenciais** do Ministério Público, incluindo sistemas de tecnologia da informação;
- c. Especificar as exigências de segurança nas cláusulas dos contratos e convênios firmados.

D 3.2 Treinamento de Segurança, conscientização e instruções

No cumprimento desse plano, o Ministério Público deve:

3.2.1- Assegurar que os membros da Instituição que possuam deveres específicos de segurança recebam treinamento apropriado, periódico e atualizado para o perfeito desempenho de suas atividades.

3.2.2- Possuir um programa de conscientização de segurança que mantenha seus integrantes conscientes de suas responsabilidades em relação à Política de Segurança da Instituição.

3.2.3- Instruir usuários, **visitantes** e prestadores de serviço a respeito de privilégios e proibições de acesso, relacionadas com a **credencial de acesso** que lhe for disponibilizada.

D 3.3 Assuntos sigilosos

3.3.1- As informações e outros assuntos cuja revelação indevida possa causar danos aos interesses Institucionais ou privados sob a responsabilidade da Instituição serão classificados de acordo com as normas vigente para salvaguarda de assuntos sigilosos.

D 3.4 Avaliação de riscos e ameaças

3.4.1- Serão conduzidas avaliações de riscos e ameaças para determinar as necessidades de proteção da Instituição, além das necessidades básicas de segurança.

a) As situações de risco serão continuamente monitoradas para fazer os ajustamentos necessários no sistema de segurança.

b) A avaliação de risco envolve:

- I. Estabelecimento do alcance da avaliação e identificação dos integrantes e bens a serem protegidos;
- II. Individualização dos riscos a integrantes e ao patrimônio e avaliação da probabilidade de confirmação e impactos no caso de concretização;
- III. Avaliação do risco baseada na existência e adequação das salvaguardas e vulnerabilidades;
- IV. Implementação de salvaguarda suplementar que elimine ou reduza o risco levantado a um nível aceitável.

D 3.5. Limitações de acesso

3.5.1- O acesso a informações e outros bens protegidos será limitado às pessoas que tenham a necessidade de conhecer ou empregar e que possuam autorização ou credencial de nível adequado.

3.5.2- Para ampliar a segurança deverá ser assegurado que nenhum indivíduo possa, de forma independente, controlar todos os aspectos de um processo ou sistema.

D 3.6 Confiabilidade da segurança

3.6.1- Deve ser assegurado que pessoas com acesso a informações e bens institucionais protegidos são dignas de confiança.

3.6.2- Deve ser assegurada a lealdade de integrantes que têm acesso a informações e bens institucionais protegidos como condição para salvaguardar a Instituição contra atividades de inteligência e terrorismo.

3.6.3- Especial cuidado deve ser tomado para prevenir atividades infiltradas e divulgação não autorizada de informações classificadas e protegidas por indivíduos em posição de confiança.

3.6.4- Deve ser assegurado que, antes de iniciar suas atividades, as pessoas que exijam acesso a:

1. bens da Instituição sejam submetidas a checagem de confiabilidade;
2. informações e bens classificados como sigilosos ou protegidos possuam *status* adequado de confiabilidade;
3. informações e bens classificados como sigilosos ou protegidos recebam credencial de segurança adequada ao nível de acesso exigido;
4. áreas e instalações controladas possuam a credencial de acesso adequada ao local.

3.6.5- Os Administradores da Instituição devem permanecer vigilantes e atuar diante de qualquer nova informação que possa colocar em questão a confiabilidade ou lealdade individual de seus administrados.

3.6.6- A confiabilidade dos dispositivos de segurança implementados deve ser regular e periodicamente verificada.

D 3.7 Segurança dos integrantes

3.7.1- A Instituição é responsável pela segurança de seus **integrantes** quando no exercício ou em função de seus cargos.

3.7.2- Essa responsabilidade abrange as situações em que seus **integrantes** estejam sob ameaça ou sofram violência em decorrência de suas atuações funcionais ou de situações de serviço às quais foram expostos.

3.7.3- Essas situações incluem, mas não são a elas limitadas, ameaça, direta ou indireta, ou sofrimento de violência ou atentado contra integrante e/ou sua família ou patrimônio.

a) Nestes casos a Instituição deve:

1. Avaliar a ameaça e o risco pelo Órgão Central responsável pela Segurança Institucional, independente das providências imediatas requeridas pela situação;
2. Identificar, proteger e dar suporte à segurança do integrante sob ameaça ou que tenha sofrido violência;
3. Investigar toda ameaça a integrantes, providenciando a resposta imediata e adequada a cada situação até sua extinção;
4. Promover informação, treinamento e aconselhamento de prevenção e procedimentos aos integrantes ameaçados.
5. Manter base de arquivos dos incidentes relatados contra **integrantes**, das avaliações realizadas, providências adotadas e resultados alcançados;
6. Avaliar as Instalações onde trabalha o **integrante** que esteja sob ameaça, implementando as necessárias salvaguardas para protegê-lo .

b) Os **integrantes** que ocupem posições de alto risco pessoal devem ser cobertos por salvaguardas adicionais, projetadas para minimizar os riscos de atentados.

c) O **integrante** ameaçado que se encontrar sob regime de proteção pela Instituição deverá comprometer-se expressamente com o atendimento das orientações do Órgão Central Responsável pela segurança e seus agentes, sendo a não-observação motivo para cessar as atividades de sua segurança.

E – DOCUMENTOS e MATERIAIS

E - 1 DOCUMENTOS

E.1.1 Produção

1.1.1- A produção de documentos com caráter de confidencialidade (secreto, confidencial e reservado) ou não, no âmbito do Ministério Público do Estado do Ceará, obedecerá a modelos internos devidamente aprovados pelos subgrupos e submetidos à aprovação do Procurador(a) Geral de Justiça.

1.1.2- As normas elaboradas para a produção de documentos sigilosos ou não, deverão conter necessariamente a obrigatoriedade de controle de segurança, **classificação ou desclassificação** e em suas elaborações e procedimentos relacionados, à identificação das partes que o compõem.

1.1.3- A guarda de documentos, com caráter de confidencialidade ou não deve ser efetuada em locais seguros e em caso de **documentos classificados** em locais de acesso restrito.

1.1.4 - Os documentos ou informações sigilosos no Ministério Público do Estado do Ceará, poderão ser classificados em **secretos, confidenciais e reservados**, em razão do seu teor ou dos seus elementos intrínsecos e receberá o status de **informação classificada**.

a) São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a ações de inteligência ou a fatos cuja divulgação sejam considerados sigilosos por lei e que precisam ser classificados para a devida remessa ou utilização judicial e cujo conhecimento não-autorizado possa acarretar dano grave à segurança pública e dos interesses institucionais.

b) Os documentos judiciais com caráter de sigilo podem receber classificação, mas sua divulgação ou desclassificação, não interferem no seu caráter de sigilo.

c) São passíveis de classificação como confidenciais dados ou informações que, no interesse do Ministério Público, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos.

d) São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

1.1.5- A remessa de documentos secretos, confidenciais e reservados deverá ser estabelecido em regulamento próprio a ser criado pelo subgrupo e seu teor submetido à aprovação do(a) Procurador(a) Geral de Justiça.

E.1.2 Recepção

1.2.1- A recepção de documentos com caráter de confidencialidade ou não, deve ser efetuada para preservar a sua **autenticidade**, **integridade** e **confidencialidade**, para que chegue ao seu local de destino e se assegure seu sigilo.

1.2.2- As áreas do Ministério Público responsáveis pela recepção de documentos com caráter de confidencialidade (secreto, confidencial e reservado) ou não, deverão ter seu corpo funcional dotado de treinamento para o recebimento de referidos documentos.

E.1.3 Difusão

1.3.1- A difusão de documentos com caráter de confidencialidade (secreto, confidencial e reservado) deverá obedecer a regras previamente estabelecidas pelo subgrupo Documentos e Materiais.

E.1.4 Destruição

1.4.1- O descarte de documentos com caráter de **confidencialidade** (secreto, confidencial e reservado) ou não obedecerá a política interna já estabelecida para tais fins, bem como as regras de arquivamento atenderá ainda as determinações do CONARQ.

E-2 MATERIAL

E-2.1 Aquisição

2.1.1- A aquisição de materiais de consumo para o Ministério Público do Estado do Ceará obedecerá às regras de licitações próprias e de *plano contínuo* de forma a evitar a descontinuidade do munus constitucional a cargo do Ministério Público.

E-2.2 Recebimento

2.2.1- Os bens e materiais adquiridos deverão ser recepcionados em um único local e devidamente tombados

E-2.3 Distribuição

2.3.1- Os bens e materiais adquiridos deverão ser, depois de recepcionados em um único local e devidamente tombados, caso necessário, remetidos ao local destinado mediante recepção do membro do Ministério Público do Estado do Ceará responsável por sua utilização ou recepção, devendo tal remessa ser precedida de registro em sistema próprio, bem como sua requisição por qualquer órgão do Ministério Público do Estado do Ceará.

E-2.4 Guarda

2.4.1- Os bens e materiais adquiridos deverão ser, depois de recepcionados em um único local e devidamente tombados, caso necessário, devidamente guardados em depósito de materiais nos prédios do Ministério Público do Estado do Ceará responsável por sua utilização ou recepção.

E-2.5 Descarte

2.5.1- O descarte de bens e materiais obedecerá a regra interna estabelecida para tais fins pelo subgrupo documentos e materiais.

REFERÊNCIAS LEGAIS

- Constituição Federal;
- Constituição do Estado do Ceará;
- Lei nº 8.625, 12 de fevereiro de 1993 - Institui a Lei Orgânica Nacional do Ministério Público;
- Lei Complementar nº 72, de - Institui a Lei Orgânica do Ministério Público do Estado do Ceará;
- Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Decreto nº 4.553, de 27 de dezembro de 2002 - Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;
- Decreto nº 5.301, de 09 de dezembro de 2004;
- Recomendação nº 13, de 16/06/2009 do Conselho Nacional do Ministério Público;
- Provimento nº 71/2008, de 18 e agosto de 2008 do Ministério Público do Estado do Ceará;
- Portaria nº 627, de 20 de outubro de 2004 do Procurador Geral da República.