

atendimento ao Ato de Segurança da Informação relacionada à utilização da Internet e, consequentemente, à Política de Segurança da Informação do Ministério Público.

Parágrafo único. Os registros de que trata o caput também podem se referir a web sites visitados, bookmarks, arquivos copiados da internet, configurações dos softwares, tempo gasto nos acessos e outras informações necessárias para a otimização dos recursos de acesso à internet e realização de auditoria.

Art. 13. As violações do presente Ato serão tratadas da seguinte forma:

I - os casos omissos devem ser tratados diretamente pelo DINF e encaminhados ao CETI;

II - não é dado ao membro, servidor ou colaborador o direito de alegar desconhecimento deste Ato; e

III - o não cumprimento do presente Ato acarretará ao membro, servidor ou colaborador as penalidades cabíveis, previstas nos âmbitos administrativo, cível e criminal.

Art. 14. Os casos omissos serão resolvidos pelo Gabinete do Procurador-Geral, ouvido o Procurador-Geral de Justiça.

Art. 15. Este Ato Normativo entra em vigor na data de sua publicação.

PUBLIQUE-SE, REGISTRE-SE E CUMPRE-SE.

GABINETE DO PROCURADOR GERAL DE JUSTIÇA, Belém, 25 de maio de 2015.

MIGUEL RIBEIRO BAIA

Procurador-Geral de Justiça, em exercício

PORTARIA Nº 3008/2015-MP/PGJ

Institui a Política de Segurança da Informação do Ministério Público do Estado do Pará.

O PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO PARÁ, no uso das atribuições que lhe são conferidas pela Lei Complementar nº 057, de 6 de julho de 2006, e

CONSIDERANDO a informação como um ativo essencial que necessita de adequada proteção aos vários tipos de ameaças externas e internas que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações do Ministério Público do Estado do Pará ou que estejam sob sua responsabilidade, visando à garantia da continuidade do negócio, à minimização de riscos e à maximização dos retornos e resultados;

CONSIDERANDO a necessidade de implementar um conjunto de controles, normas, procedimentos, padrões e sistemas que visem ao estabelecimento, à implantação, ao monitoramento, à análise e ao melhoramento contínuo da segurança da informação;

CONSIDERANDO a crescente importância e o reconhecimento da segurança da informação, que suscita a perquirição sobre um ambiente seguro, a melhoria dos processos de trabalho, a adoção de novas tecnologias e, sobretudo, a conscientização e educação das pessoas,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação do Ministério Público do Estado do Pará, com a finalidade de estabelecer diretrizes de segurança da informação, visando à adoção de procedimentos e mecanismos relacionados à proteção das informações de sua propriedade e sob sua guarda, a serem cumpridos por seus membros, servidores e colaboradores.

Parágrafo único. A estrutura da Política de Segurança da Informação do Ministério Público do Estado do Pará compreende:

I - a Política de Segurança da Informação (Política): instituída por este Ato Normativo, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação e deve ser revisada anualmente pelo Comitê Estratégico de Tecnologia da Informação (CETI);

II - as Normas de Segurança da Informação (Normas): instituídas pelas diretorias das áreas envolvidas, estabelecem obrigações e procedimentos, definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada, e devem ser revisadas anualmente pelas diretorias das áreas envolvidas e aprovadas pelo CETI; e

III - os Procedimentos de Segurança da Informação (Procedimentos): instituídos pelo nível gerencial, instrumentalizam o disposto nas Normas e na Política, permitindo a sua direta aplicação nas atividades do Ministério Público do Estado do Pará, devendo ser revisados anualmente, diretamente pelos níveis gerenciais das áreas envolvidas.

Art. 2º Para efeito do disposto neste Ato Normativo, considera-se:

I - ameaça: agente ou ação, espontânea ou proposital, que afeta um sistema por meio de suas vulnerabilidades, causando prejuízos e/ou redução de disponibilidade;

II - ativos de tecnologia da informação: estações de trabalho, servidores, software, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação, bem como conexões com a internet, hardware e software;

III - auditoria: análise crítica do sistema de gestão de segurança da informação, em que são verificadas a conformidade dos controles implementados e a eficácia de seu atendimento;

IV - backup: cópia de segurança gerada para possibilitar o acesso e recuperação futura das informações;

V - confidencialidade: proteção às informações contra

o acesso de qualquer pessoa não autorizada pelo gestor da informação;

VI - continuidade do negócio: capacidade estratégica e tática da Instituição de se planejar e responder a incidentes e interrupções de negócios para conseguir continuar suas operações em um nível aceitável e previamente definido;

VII - controle: qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco, podendo ser de natureza administrativa, técnica, de gestão ou legal;

VIII - disponibilidade: garantia de que o serviço esteja funcionando conforme especificado e o acesso às informações esteja disponível somente a usuários autorizados;

IX - firewall: sistema de segurança de computadores usado para restringir o acesso de/para em uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas;

X - gestão de risco: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, abrangendo, inclusive, a análise e a avaliação, o tratamento, a aceitação e a comunicação dos riscos;

XI - hardware: parte física dos equipamentos tecnológicos, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos;

XII - incidente de segurança da informação: representado por um simples evento ou por uma série de eventos de segurança da informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XIII - integridade: inteireza que deve ser garantida a toda informação trafegada ou armazenada, de forma a assegurar que ela não seja indevidamente alterada ou eliminada;

XIV - Norma de Segurança da Informação (Norma): documento que estabelece obrigações e requisitos de segurança a serem seguidos por todos os usuários, de acordo com as diretrizes da Política de Segurança da Informação;

XV - processo: conjunto de atividades inter-relacionadas com um objetivo específico que pode ser a criação de um produto ou serviço;

XVI - processos de negócio: atividade finalística de uma organização para geração de produtos ou serviços;

XVII - proprietário da informação: todo aquele responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à Instituição ou sob a sua guarda;

XVIII - segurança da informação: conjunto de processos articulados que busca a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno dos ganhos sobre os investimentos;

XIX - request for comments (RFC): fonte de informação padrão no que diz respeito à descrição de métodos, ao comportamento, à pesquisa ou à inovação aplicável à internet e/ou a sistemas a ela relacionados;

XX - risco: combinação de sequências de um evento e a probabilidade de ocorrência associada;

XXI - software: é a manipulação, a instrução de execução, o redirecionamento e a execução de atividades lógicas dos equipamentos de tecnologia da informação;

XXII - terceiro: qualquer parceiro, fornecedor ou prestador de serviço que acesse informações ou utilize recursos de tecnologia da informação disponibilizados pelo Ministério Público do Estado do Pará;

XXIII - usuário: qualquer colaborador, seja ele servidor, estagiário, parceiro, fornecedor, prestador de serviço ou terceiro em geral, que acesse ou utilize informações custodiadas ou de propriedade do Ministério Público do Estado do Pará; e

XXIV - vulnerabilidade: fragilidade de um software, sistema operacional ou outro componente da infraestrutura de tecnologia da informação que pode ser explorada por uma ou mais ameaças.

Art. 3º São diretrizes básicas da Política de Segurança da Informação do Ministério Público do Estado do Pará:

I - responsabilidade pela garantia da segurança, do controle e da administração das informações da Instituição;

II - a informação produzida ou recebida é de propriedade do Ministério Público, devendo ser armazenada e protegida quanto ao seu acesso e uso e classificada quanto à sua integridade, confidencialidade e disponibilidade;

III - o acesso às informações de propriedade do Ministério Público será direcionado ao desempenho das atividades ministeriais e plenamente adequado aos objetivos institucionais;

IV - responsabilidade dos membros, servidores e colaboradores do Ministério Público pelo cumprimento da Política de Segurança da Informação;

V - alinhamento das normas, dos procedimentos e planos de implantação, da gestão e da auditoria de segurança da informação institucional com a Política de Segurança da Informação;

VI - divulgação ampla e irrestrita da Política de Segurança da Informação;

VII - vedação do uso de informações de propriedade do

Ministério Público para interesses que não estejam de acordo com os objetivos institucionais;

VIII - responsabilidade pela realização e acompanhamento das manutenções preventivas periódicas dos equipamentos e instalações, visando à preservação do patrimônio institucional;

IX - ambiente tecnológico mantido, atualizado e supervisionado, de modo a atender os níveis e requisitos de segurança próprios e inerentes às funções institucionais; e

X - definição de responsabilidades e sanções, nos casos de violação da Política de Segurança da Informação, para membros, servidores e colaboradores do Ministério Público.

Art. 4º São diretrizes relativas ao ambiente e acesso físico:

I - desenvolvimento de planos específicos que englobem a plena conservação do ambiente físico do Ministério Público;

II - controle do acesso físico às dependências e instalações do Ministério Público, disciplinando a circulação de pessoas, materiais e equipamentos;

III - recursos e instalações críticas ou sensíveis protegidos física e adequadamente contra riscos identificados, acessos não autorizados, danos ou interferências, por meio de barreiras de segurança e controles de acesso;

IV - acessos aos painéis de controle e cabamentos de energia e de comunicação restritos aos técnicos e profissionais das áreas de segurança, engenharia e de infraestrutura;

V - registro e atualização sistemáticos, em período predefinido, do inventário do conjunto de ativos relevantes, sensíveis e críticos para a Instituição;

VI - localização das instalações sensíveis e críticas, não identificável publicamente;

VII - exigência de autorização formal para executar intervenções e manutenções no ambiente físico do Ministério Público, as quais deverão estar submetidas a uma supervisão previamente responsabilizada;

VIII - exigência de áreas de limite (perímetro) de segurança para todas as instalações do Ministério Público;

IX - exigência de instalações apropriadas para guarda, utilização e lotação dos recursos tecnológicos e materiais;

X - instalações e equipamentos adequados à integridade de membros, servidores e colaboradores;

XI - estabelecimento de normas e procedimentos para triagem de documentos em qualquer suporte, antes de seu descarte, reciclagem ou reutilização;

XII - equipamentos apropriados e pessoal treinado para o combate a incêndio, compatíveis com a área, espaço físico e instalação a ser protegida; e

XIII - utilização de equipamentos de combate a incêndio, quando necessário, de acordo com treinamentos e seguindo instruções do fabricante.

Art. 5º São diretrizes relativas à segurança em recursos humanos:

I - obediência aos dispositivos legais para a seleção, a nomeação e a contratação de profissionais, considerando as competências de caráter pessoal, profissional e acadêmico;

II - responsabilização dos profissionais de níveis hierárquicos superiores pela supervisão da conduta e do comportamento de seus subordinados (diretos e indiretos), identificando as ocorrências que possam comprometer a segurança da informação;

III - compromisso de confidencialidade e de cumprimento da Política, das Normas e dos Procedimentos de Segurança da Informação do Ministério Público, com previsão de sanções e penalidades em caso de violação das regras;

IV - ampla divulgação, entre membros, servidores e colaboradores do Ministério Público, das medidas e procedimentos que eliminem riscos de acessos não autorizados, perdas, danos e violações de segurança, com relação aos ativos tangíveis e intangíveis da Instituição;

V - obrigatoriedade do porte e do uso de identificação funcional durante a permanência de servidores e colaboradores nas dependências, instalações e unidades do Ministério Público;

VI - identificação de membros, servidores, colaboradores e visitantes, imprescindível, pessoal e intransferível, responsabilizando-os pelas ações praticadas por meio dela;

VII - treinamento e atualização sistemática de membros, servidores e colaboradores do Ministério Público em políticas, normas e procedimentos de segurança da informação, visando ao pleno exercício de suas funções;

VIII - responsabilidade pessoal e intransferível pelo sigilo, privacidade e uso de senhas de acesso aos recursos computacionais, não podendo ser compartilhadas, divulgadas, anotadas em papel ou em sistema visível ou de acesso não protegido;

IX - troca imediata das senhas, nos casos de perda de sigilo ou mesmo suspeita;

X - bloqueio imediato dos acessos aos recursos tecnológicos com perfil de usuário, nos casos de exoneração, aposentadoria e desligamentos de qualquer natureza;

XI - previsão formal e contratual de cuidados e responsabilização quanto à segurança dos ativos do Ministério Público, nas contratações de prestação de serviços;