Diário Oficial
Ano LXXXIX - Recife, quarta-feira, 10 de outubro de 2012 - Nº 193

SECRETARIA DE DEFESA SOCIAL

PORTARIA GAB/SDS N° 3081, de 09/10/2012

O SECRETÁRIO DE DEFESA SOCIAL, no uso das atribuições que lhe são conferidas pelos incisos III do art. 42 da Constituição do Estado de Pernambuco, a Lei Complementar nº 049/2003, artigo 3º, inciso IV e a Lei nº 14.264/2011, no seu artigo 1º, inciso VII, e, **CONSIDERANDO** que o uso da tecnologia da informação na Secretaria de Defesa Social envolve grande acervo de recursos computacionais e informações que necessitam estar permanentemente protegidos contra acessos indevidos e adulterações;

CONSIDERANDO a necessidade de estabelecer diretrizes e valores para a gestão de segurança da informação e comunicações digitais no âmbito da Secretaria de Defesa Social;

CONSIDERANDO a importância que deve ser dada ao esforço pela integridade, disponibilidade, confidencialidade e à autenticidade dos dados e das informações nos mais diversos suportes utilizados por esta Secretaria;

CONSIDERANDO os padrões nacionais e internacionais constantes nas Normas NBR ISO/IEC 27001, que versa sobre sistemas de gestão de segurança da informação, e NBR ISO/IEC 27002, atinente ao Código de Prática para a Gestão da Segurança da Informação;

CONSIDERANDO as disposições constantes na Norma Técnica da Agência de Tecnologia da Informação - ATI-SGRPR/ 001:10, que estabelece as diretrizes gerais da Política de Segurança da Informação, **RESOLVE**:

Art.1º Instituir, no âmbito da Secretaria de Defesa Social e de seus Órgãos subordinados (doravante denominados indistintamente por Secretaria de Defesa Social), a Política de Segurança das Informações Digitais, regida pelos objetivos e diretrizes estabelecidos nesta Portaria, e **criar** o Comitê Gestor de Segurança da Informação Digital com as atribuições descritas adiante;

Art. 2º Para efeitos desta Portaria, adotam-se os seguintes conceitos:

I - acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

II - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na Secretaria de Defesa Social e equipara-se a quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no âmbito da Secretaria de Defesa Social;

III - ameaça: evento que tem potencial para comprometer os objetivos da organização, pela exploração de uma vulnerabilidade de qualquer natureza, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - ativo de informação: ativo que guarda informações do órgão;

VI - auditoria: atividade com a finalidade de escrutinar, e eventualmente reconstruir, um evento relacionado à segurança para auxiliar no exame de suas causas e efeitos;

VII - autenticar: processo que busca verificar a identidade de uma pessoa no momento em que é requisitado um acesso a determinado ambiente ou recurso de tecnologia da informação;

VIII - cessão de bases de dados: ato de disponibilizar cópia, total ou parcial, de dados da Secretaria de Defesa Social, aprovada pelo gestor competente;

IX - ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando seus requisitos de confidencialidade, integridade e disponibilidade;

X - classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

XI - concedente: responsável pelo fornecimento da base de dados confidenciais pela Secretaria de Defesa Social;

XII - confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIII - conta de acesso: conjunto do “nome de usuário” e “senha”, ou outros recursos para identificação e autenticação, utilizado para acesso aos sistemas informatizados e recursos de tecnologia da informação e comunicação;

XIV - controles de segurança: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XV - custodiante: agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

XVI - dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVII – dados confidenciais: dados pessoais que permitam a identificação da pessoa e possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas e religiosas, crenças, ideologia, saúde física, saúde mental, vida sexual, registros policiais, assuntos familiares, profissão e outros que a lei assim o definir, não podendo ser divulgados ou utilizados para finalidade distinta da que motivou a estruturação do banco de dados, salvo por ordem judicial ou com anuência expressa do titular ou de seu representante legal;

XVIII - dados pessoais: representação de fatos, juízos ou situações referentes a uma pessoa física ou jurídica, passível de ser captada, armazenada, processada ou transmitida por meios informatizados ou não;

XIX - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XX - documento confidencial: contém informações que, no interesse do Poder Executivo Estadual e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado;

XXI - evento: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação;
XXII - gestor da informação: agente público da Secretaria de Defesa Social responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;
XIII - grau de sigilo: gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo;
XXIV - incidente de segurança: todo e qualquer evento adverso, confirmado ou sob sus peita, relacionado à segurança de sistemas de informação ou de redes de computadores;
XXV - informação custodiada: informação sob a guarda e responsabilidade de alguém;
XXVI - integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
XXVII - logs: arquivos em computador utilizados para manter registros das atividades executadas por programas e usuários nos computadores e sistemas informatizados;
XXVIII - recursos de tecnologia da informação e comunicação: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, *smartfones*, servidores de rede, equipamentos de conectividade e infra-estrutura;
XXIX - rede corporativa: conjunto de todas as redes locais sob a gestão da Secretaria de Defesa Social, não importando o meio ou forma de transmissão;
XXX - rede local: conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários de rede da Secretaria de Defesa Social;
XXXI - segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação e, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas, conforme o caso;
XXXII - senha ou credencial: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;
XXXIII - sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada;
XXXIV - software: programa de computador desenvolvido ou adquirido para executar um conjunto de ações previamente definidas;
XXXV - usuário da rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa da Secretaria de Defesa Social;
XXXVI - usuário de sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pela Secretaria de Defesa Social; e
XXXVII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

TÍTULO I
DA POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES DIGITAIS
CAPÍTULO I
Dos objetivos

Art. 3º Esta política aplica-se ao ambiente de trabalho e aos recursos de tecnologia da informação e comunicação, estabelecendo responsabilidades e obrigações a todos os que tenham acesso às informações ou aos recursos de tecnologia da informação e comunicação da Secretaria de Defesa Social e de seus órgãos subordinados.
Art. 4º Constituem objetivos da política:
I - estabelecer suas diretrizes, a serem seguidas pela Secretaria de Defesa Social e seus colaboradores no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações; **II** - prover a Secretaria de Defesa Social de normas para a segurança da informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizados a dados e informações; e
III - definir um conjunto de instrumentos normativos e organizacionais que capacitem a Secretaria de Defesa Social a assegurar a confidencialidade, a integridade e a disponibilidade dos dados e das informações.

CAPÍTULO II
Das Diretrizes

Art. 5º A Política rege-se pelas seguintes diretrizes:
I - propriedade da informação:
a) toda informação criada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos da Secretaria de Defesa Social, no exercício de suas atividades, é de propriedade do órgão e deve ser protegida segundo as diretrizes aqui descritas e as regulamentações em vigor; **b)** a informação custodiada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos, no exercício de suas atividades, deve ser protegida segundo as diretrizes aqui descritas e nas demais regulamentações em vigor; **c)** quando da obtenção de informação de terceiros, o Gestor da Informação deve providenciar junto ao concedente a documentação formal que atenda aos direitos de acesso antes de seu uso; **d)** na cessão de bases de dados nominais custodiadas ou na informação de propriedade da Secretaria de Defesa Social a terceiros, o Gestor da Informação deve providenciar a documentação formal relativa à autorização de acesso às informações.
II - **classificação da informação**:
a) toda informação criada, manuseada, armazenada, transportada ou descartada pela Secretaria de Defesa Social deve ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita, conforme legislação vigente;
b) um processo de classificação da informação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade da Secretaria de Defesa Social ao longo do seu ciclo de vida;
c) toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pela Secretaria de Defesa Social é de sua responsabilidade e deve ser protegida, adequadamente, conforme a classificação das informações;
d) a classificação da informação é atribuição do Gestor da Informação, observadas as formalidades legais.

III - **permissão de acesso:**
a) todos os recursos de tecnologia da informação e comunicação sob responsabilidade da Secretaria de Defesa Social deve ter um Gestor formalmente designado por autoridade competente; **b)** o agente público que utiliza os recursos de tecnologia da informação e comunicação deve ter uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;
c) os privilégios de leitura, modificação ou eliminação das informações devem ser definidos pelo Gestor da Informação;
d) a autorização, o acesso, o uso da informação e dos recursos de tecnologia da informação e comunicação devem ser controlados e limitados ao cumprimento das atribuições de cada agente público e qualquer outra forma de uso necessita de prévia autorização formal pelo Gestor da Informação;
e) sempre que houver mudanças nas atribuições de determinado agente público, será de responsabilidade da chefia imediata informar os seus privilégios de acesso às informações e aos recursos de tecnologia da informação e comunicação para que sejam adequados imediatamente; **f)** no caso de exoneração ou demissão, esses privilégios devem ser cancelados;
IV - **Gestão de Continuidade de Negócio:**
a) deve ser estabelecida a Gestão de Continuidade de Negócio em segurança da informação e comunicações no âmbito da Secretaria de Defesa Social, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de tecnologia da informação e comunicação que suportam as operações;
b) deve ser estabelecido um processo de gestão de risco com vistas a minimizar possíveis impactos associados aos ativos, processo esse que deve possibilitar a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;
c) as medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança;
d) toda informação institucional, se eletrônica, deve ser armazenada nos servidores de arquivo da rede corporativa e, se não eletrônica, deve ser mantida em local que a salvaguarde adequadamente;
e) no descarte de informações institucionais devem ser observados as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação;
f) os recursos de tecnologia da informação e comunicação disponibilizados para criação, manuseio, armazenamento, transporte e descarte da informação na Secretaria de Defesa Social devem dispor de mecanismos que minimizem os riscos inerentes a problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios da integridade, da disponibilidade e da confidencialidade das informações;
g) os recursos de tecnologia da informação e comunicação utilizados devem ser previamente homologados, identificados individualmente e inventariados, além de possuir documentação mínima e atualizada para o seu uso e estar em conformidade com as normas de segurança especificas;
V - **monitoramento:**
a) o uso dos recursos de tecnologia da informação e comunicação disponibilizados é passível de monitoramento e auditoria;
b) a entrada e a saída de ativos de informação nas dependências da Secretaria de Defesa Social devem ser registradas e autorizadas por autoridade competente.

TÍTULO II
DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DIGITAL
CAPÍTULO I
Da composição

Art. 6º O Comitê Gestor de Segurança da Informação Digital da Secretaria de Defesa Social é composto pelos seguintes grupos:
I – Deliberativo;
II – Técnico.
Art. 7º Integram o grupo deliberativo:
I – O Secretário Executivo de Defesa Social (Presidente);
II – O Comandante Geral da Polícia Militar;
III - O Comandante Geral do Corpo de Bombeiros Militar;
IV – Chefe da Polícia Civil;
V – Gerente Geral de Polícia Científica.
Art. 8º Integram o grupo técnico:
I – Secretário Executivo de Gestão Integrada (Coordenador);
II – Gerente de Tecnologia da Informação (Auxiliar);
III - Gerente Geral de Assuntos Jurídicos (GGAJ);
IV - Gerente do Centro Integrado de Inteligência de Defesa Social (CIIDS);
V – Gerente Geral do Centro Integrado de Operações de Defesa Social (CIODS);
VI – Superintendente de Gestão de Pessoas (SGP);
VII – Perito em computação forense do Instituto de Criminalística;
VIII – Um representante de cada Órgão Operativo.

CAPÍTULO II
Das atribuições

Art. 9º Compete ao grupo deliberativo:
I – Através do Secretário Executivo de Defesa Social, convocar o Comitê caso instado pelo Secretário de Defesa Social ou por demandas do próprio Comitê;
II - Aprovar e revisar as diretrizes da política e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações da Secretaria de Defesa Social;
III – Executar as atribuições do Comitê Gestor de Segurança da Informação Digital da Secretaria de Defesa Social, como disposto neste diploma;
IV – Determinar a agenda do grupo técnico pelo encaminhamento de demandas de sua competência;
V- Apreciar, e eventualmente ratificar, estudos e pareceres emitidos pelo grupo técnico;
VI – Informar e encaminhar ao Secretário de Defesa Social sobre as questões de competência do Comitê.

Art. 10 Compete ao grupo técnico:
I – Analisar e elaborar estudos e pareceres acerca de questões técnicas alusivas a Segurança de Informações Digitais;
II – Analisar e emitir parecer acerca de solicitações de acessos a dados e recursos de Tecnologia da informação, originárias de órgãos externos à Secretaria de Defesa Social;
III – Elaborar as normas disciplinares alusivas as seguintes matérias:
a) a criação e manutenção de contas e acesso à informação e aos recursos de tecnologia da informação e comunicação;
b) o uso do correio eletrônico;
c) uso aceitável dos recursos de tecnologia da informação;
d) a cessão de bases de dados e outras informações;
e) o uso da Internet no ambiente da Secretaria de Defesa Social;
f) o controle de acesso lógico e remoto;
g) a segurança da informação para técnicos;
h) a segurança para estações de trabalho e equipamentos eletrônicos portáteis;
i) a segurança física de instalações que alocam recursos de tecnologia da informação;
j) a instalação e configuração de aplicações para produção;
k) o tratamento de mídias e cópias de segurança;
l) o projeto e desenvolvimento de aplicações;
m) a segurança contra código malicioso;
n) o aculturamento do elemento humano;
o) a segurança em contratos de prestação de serviços;
p) a segregação de função;
q) o registro de eventos e trilhas de auditoria;
r) o gerenciamento de vulnerabilidades;
s) os procedimentos para custódia de equipamentos; e
t) o termo de responsabilidade.
IV – Submeter, para apreciação do grupo deliberativo, sugestões para o aprimoramento da Segurança da Informação Digital, nos âmbitos de gestão e operacional.
V – Assessorar e apoiar o grupo deliberativo nas questões técnicas sempre que instado.

TÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 11 As diretrizes de segurança da informação estabelecidas nesta Portaria aplicam-se às informações armazenadas, bem como às que estão sendo transmitidas, e devem ser seguidas pelos agentes públicos, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.
Art. 12 A política deve ser difundida a todos os agentes públicos por um processo permanente de aculturamento e conscientização em segurança da informação.
Art. 13 É dever do agente público conhecer, cumprir e fazer cumprir a Política de Segurança da Informação.
Art. 14 É condição para acesso aos ativos de informação a adesão formal aos termos desta Portaria.
Art. 15 O agente público é responsável pela segurança dos ativos de informação e processos que estejam sob a sua responsabilidade.
Art. 16 Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação devem receber capacitação especializada.
Art. 17 Os contratos firmados pela Secretaria de Defesa Social devem conter cláusulas, ou serem aditivados, de forma que determinem a observância desta política e normas dela derivadas por terceiros de qualquer natureza.
Art. 18 Os recursos de tecnologia da informação e comunicação disponibilizados pela Secretaria de Defesa Social devem ser utilizados estritamente dentro do seu propósito, constituindo falta grave sua inobservância.
Parágrafo único. É vedado, a qualquer agente público, o uso dos recursos de tecnologia da informação e comunicação para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela Secretaria de Defesa Social e órgãos associados ou para perpetrar ações que, de qualquer modo, venham a constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, nacional ou estrangeira, assim como àquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem do órgão.
Art. 19 Os agentes públicos devem reportar formalmente à Gerência de Tecnologia da Informação os incidentes, ou evidências que suscitem suspeitas, que possam afetar a segurança dos ativos ou o descumprimento da política. **Art. 20** Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação e comunicação, a Gerência de Tecnologia da Informação deverá ser imediatamente acionada para tomar as providências necessárias a fim de sanar as causas, podendo, inclusive, determinar a restrição temporária do acesso às informações ou ao uso dos recursos de tecnologia da informação e comunicação, conforme o caso.
Art. 21 A violação das normas de segurança da informação resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de tecnologia da informação e comunicação, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas cíveis e penais cabíveis. **Art. 22** Os casos omissos serão resolvidos pelo Secretário de Defesa Social, ou seu substituto legal, assessorados pelo Comitê Gestor de Segurança da Informação Digital.
Art. 23 O Comitê Gestor de Segurança
da Informação Digital deverá revisar, sempre que necessário, a política e todos os atos normativos dela decorrentes, não excedendo o período máximo de 2 (dois) anos.
Art. 24 Esta Portaria entra em vigor na data de sua publicação.
Art. 25 Ficam revogadas as disposições em contrário. Recife, 09 de outubro de 2012.

WILSON SALLES DAMÁZIO
Secretário de Defesa Social.