ATO DPG Nº 014, DE 04 DE JUNHO DE 2018.

Institui a Política de Segurança da Informação (PSI) no âmbito da Defensoria Pública do Estado de Santa Catarina.

Considerando as diretrizes contidas na 4ª edição do manual de Boas Práticas em Segurança da Informação publicado pelo Tribunal de Contas da União (TCU), a recomendar a implantação, pelos órgãos e instituições públicas, de uma Política de Segurança da Informação (PSI);

Considerando a necessidade de se criar mecanismos para garantir os direitos individuais e coletivos dos integrantes e usuários do serviço público referentes à inviolabilidade da sua intimidade e ao sigilo do trâmite e armazenamento das informações;

Considerando a permanente meta de aperfeiçoar o desempenho da rede local, de otimizar a utilização da memória e da capacidade de armazenamento de dados digitais, bem como de controlar o custo financeiro na utilização dos serviços e dos recursos de tecnologia da informação; e

Considerando a proposta da Comissão Especial para a Implantação da Política de Segurança da Informação (PSI), instituída pela Portaria nº 11 de 02/02/2018 (DOE/SC nº 20.706 de 07/02/2018), constituída com o fim de realizar estudos para implantar, divulgar e operacionalizar a Política de Segurança da Informação da Defensoria Pública do Estado de Santa Catarina;

A **DEFENSORA PÚBLICA-GERAL DO ESTADO DE SANTA CATARINA**, no uso das atribuições contidas no Artigo 10, Incisos I e XIII da Lei Complementar nº 575, de 2 de agosto de 2012, resolve instituir, nos termos adiante expostos, a Política de Segurança da Informação da Defensoria Pública do Estado de Santa Catarina.

CAPÍTULO I - DA DISPOSIÇÃO PRELIMINAR

Art. 1º. Este Ato institui a Política de Segurança da Informação - PSI da Defensoria Pública do Estado de Santa Catarina – DPE/SC.

CAPÍTULO II – DOS FUNDAMENTOS

Art. 2º. A Política de Segurança da Informação tem como principais fundamentos:

I – a garantia aos direitos individuais e coletivos dos integrantes e usuários do serviço público referentes à inviolabilidade da sua intimidade e ao sigilo do trâmite e armazenamento das informações;

II – a proteção de assuntos que, sob à ótica dos direitos fundamentais, reclamem tratamento especial;

III – a utilização dos mecanismos da tecnologia da informação com responsabilidade e segurança;

IV – o desenvolvimento de mecanismos de segurança da informação;

V – a correta utilização das tecnologias da informações sensíveis e duais; e

VI – a conscientização dos Órgão de Atuação e Execução sobre a importância das informações processadas e armazenadas e o respectivo risco do manuseio incorreto ou inadequado.

CAPÍTULO III – DOS OBJETIVOS

Art. 3º. São objetivos da Política de Segurança da Informação:

I – propiciar o acesso institucional a instrumentos que assegurem a legalidade, confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tramitadas e/ou armazenadas, classificadas e sensíveis;

II – viabilizar a realização de auditorias nas informações tramitadas e/ou armazenadas;

III – capacitar os usuários das ferramentas derivadas da tecnologia da informação;

IV – instituir procedimentos e formulários referentes às demandas ligadas à tecnologia da informação;

V – aprimorar a tramitação e o armazenamento das informações institucionais; e

VI – viabilizar a evolução dos instrumentos de tramitação e armazenamento de informações.

CAPÍTULO IV – DOS CONCEITOS

Art. 4º. A Política de Segurança da Informação utilizará os seguintes conceitos:

I – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

II – Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com as normas legais e institucionais.

III – Recursos Tecnológicos Institucionais: equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pela DPE/SC, tais como: a) equipamentos de informática de qualquer espécie; b) impressoras; c) equipamentos de redes; d) equipamentos de telecomunicações de qualquer espécie, incluindo celulares corporativos e modens 3G; e e) recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, dados corporativos, documentos, programas ou *hardware*, arquivos de configuração que são armazenados, executados ou transmitidos através da infraestrutura computacional da DPE/SC, redes ou outros sistemas de informação;

IV – Usuário: qualquer pessoa, física ou jurídica, com vínculo oficial com a Defensoria Pública ou em condição autorizada que utiliza, de qualquer forma, algum recurso ligado à Instituição, especialmente os Defensores Públicos, Servidores, Estagiários, prestadores de serviços e fornecedores da Instituição;

V – Dado: informação sobre fatos, incluindo medidas, declarações e estatísticas;

VI - Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações; e

VII – Dado de Uso Institucional: todos os dados capturados e utilizados nas operações de serviço e administrativas, incluindo dados: a) de recursos humanos; b) financeiros; c) de equipamentos de qualquer natureza; d) de políticas, procedimentos e manuais; e e) de páginas Web.

CAPÍTULO V – DA IMPLEMENTAÇÃO DA PSI

Art. 5º. A Política de Segurança da Informação será implementada pela Gerência de Tecnologia da Informação e Gestão Eletrônica - GETIG.

Parágrafo único. A Diretoria-Geral Administrativa acompanhará a implementação da PSI na atividade administrativa e a Corregedoria-Geral supervisionará a implementação na atividade finalística.

Art. 6º. Sem prejuízo da adoção das demais medidas necessárias à implementação da PSI, incumbe à GETIG:

I – elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos da PSI;

II – sugerir providências destinadas à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;

III – acompanhar a evolução tecnológica das atividades inerentes à segurança da informação;

IV – realizar auditorias objetivando aferir o nível de segurança dos respectivos sistemas de informação;

V – estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos critptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os sistemas de segurança da informação;

VI – sugerir a adoção de procedimentos referentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;

VIII – desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações; e

IX – propor alterações deste Ato e de outras normas referentes à segurança da informação.

CAPÍTULO VI – DA UTILIZAÇÃO DOS RECURSOS

Art. 7º. Os recursos tecnológicos institucionais serão utilizados conforme exposto nas seções integrantes deste Capítulo.

SEÇÃO I – DO *ACTIVE DIRECTORY*

Art. 8º. As informações institucionais da DPE/SC serão armazenadas no *Active Directory,* sendo vedada, para este fim, a utilização de redes ou locais paralelos.

§ 1º. O *Active Directory* destina-se exclusivamente ao armazenamento de informações institucionais, sendo vedada sua utilização para fins pessoais.

§ 2º. A GETIG informará aos usuários os locais destinados ao armazenamento das informações tramitadas, bem como expedirá as orientações necessárias.

§ 3º. A GETIG auditará o *Active Directory* periodicamente e, a partir das auditorias, sugerirá medidas para aprimorar a sua utilização.

SEÇÃO II – DO CORREIO ELETRÔNICO

Art. 9º. Os usuários são responsáveis pelas respectivas contas de e-mail institucional, que deverão ser utilizadas exclusivamente para a prestação do serviço público de orientação e assistência jurídica aos vulneráveis e para comunicações institucionais e administrativas entre os usuários.

§ 1º. O endereço de e-mail corporativo da Defensoria Pública é de uso exclusivamente institucional, sendo vedada a sua utilização em sistemas de correntes, em redes sociais ou para criar fóruns eletrônicos de assuntos diversos daqueles inerentes à atividade exercida pelo usuário.

§ 2º. Quanto às solicitações relativas a demandas administrativas, devem os usuários atentar para que o seu direcionamento seja enviado para os setores com atribuição para respondê-las, conforme as funções previstas no Regimento Interno da Defensoria Pública.

§ 3º. A utilização indevida do e-mail será apurada consoante as normas institucionais.

Art. 10. A GETIG estabelecerá a capacidade de armazenamento das contas de e-mail, expedirá as orientações necessárias à correta utilização e efetuará cópias de segurança sempre que tal providência for determinada pelo Defensor Público-Geral ou pelo Corregedor-Geral.

Art. 11. É assegurada a inviolabilidade do conteúdo das mensagens que contenham informações referentes aos assistidos, exceto em casos de ordem judicial em sentido diverso.

Parágrafo único. A restrição prevista no Artigo anterior não se aplica aos Órgão da Administração Superior.

SEÇÃO III – DA *INTERNET WEB*

Art. 12. O acesso à *internet* web por intermédio dos recursos tecnológicos institucionais será assegurado e monitorado pela GETIG, que assegurará a privacidade e a confiabilidade das informações.

§ 1º. A GETIG poderá estabelecer protocolos de acesso e instituir a utilização de *login* e senha.

§ 2º. O acesso às páginas da *internet* tem caráter funcional e deve servir apenas como subsídio para execução de rotinas de trabalho de cada área, ou como fonte de pesquisa/consulta de informações relativas à atividade laboral.

§ 3º. O acesso às páginas da *internet* será monitorado por amostragem pela GETIG, com a possibilidade de emissão de relatórios, retratando o uso pelo usuário e em caso de uso indevido do recurso, a GETIG encaminhará para a Corregedoria-Geral.

SEÇÃO IV – DAS IMPRESSÕES

Art. 13. A GETIG monitorará a utilização das impressoras e emitirá os relatórios correspondentes.

Parágrafo único. O monitoramento tem por objetivo a construção e implementação de política que assegure a correta utilização dos recursos institucionais e evite a indevida publicização de dados dos usuários do serviço prestado pela Instituição.

SEÇÃO V – DOS *SOFTWARES*

Art. 14. A GETIG listará, divulgará e instalará os *softwares* que podem ser utilizados no âmbito institucional.

Parágrafo único. A instalação de quaisquer *softwares* ou programas nos computadores institucionais por terceiros dependerá de autorização da GETIG.

SEÇÃO VI – DAS SENHAS

Art. 15. As senhas e demais permissões de acesso são pessoais e intransferíveis.

Parágrafo único. A GETIG expedirá as orientações necessárias sobre a guarda e a utilização das senhas e permissões de acesso e definirá os níveis de acesso aos recursos tecnológicos institucionais.

SEÇÃO VII – DA UTILIZAÇÃO DE RECURSOS PESSOAIS

Art. 17. A utilização de recursos tecnológicos pessoais no âmbito da Defensoria Pública somente será permitida após a autorização da GETIG, que estabelecerá o procedimento de tramitação dos respectivos pedidos.

CAPÍTULO VII – DAS DISPOSIÇÕES FINAIS

Art. 18. Os administradores e os usuários dos recursos tecnológicos institucionais deverão empreender esforços para a sua correta utilização.

Parágrafo único. As dúvidas acerca da utilização dos recursos institucionais tecnológicos, especialmente àquelas relacionadas à utilização imprópria, serão solucionadas pela GETIG na forma e nos prazos das normas institucionais.

Art. 19. Fica proibido o uso dos recursos tecnológicos institucionais disponibilizados para fins particulares ou atividades que não estejam diretamente ligadas às atribuições funcionais ou, ainda, utilizá-los de forma que prejudiquem a imagem da Defensoria Pública de Santa Catarina.

Parágrafo único. Não será permitido manter armazenados dados que não sejam pertinentes às atividades de trabalho, arquivados nos servidores da rede.

Art. 20. Este Ato entra em vigor na data de sua publicação.

Florianópolis/SC, 04 de junho de 2018.

ANA CAROLINA DIHL CAVALIN
Defensora Pública-Geral