PROCURADORIA-GERAL DE JUSTIÇA
RESOLUÇÃO Nº 1.521/2022-PGJ, DE 20 DE SETEMBRO DE 2022.
(SEI Nº 29.0001.0202346.2021-85)

Institui a Política de Segurança da Informação do Ministério Público de São Paulo.

O **PROCURADOR-GERAL DE JUSTIÇA**, no uso de suas atribuições legais,

CONSIDERANDO a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), a Lei n° 12.965/2014 (Lei do Marco Civil da Internet), a Lei n° 12.527/2011 (Lei de Aceso à Informação), a Lei n° 8.625/1993 (Lei Orgânica Nacional do Ministério Púbico), a Lei Complementar Estadual n° 734/1993 (Lei Orgânica do Ministério Público do Estado de São Paulo) e a Resolução n° 1.299/2021 - PGJ, de 13 de janeiro de 2021, bem como as boas práticas de governança de dados e segurança da informação;

CONSIDERANDO o investimento e as ações para a modernização do Ministério Público de São Paulo e de sua infraestrutura de tecnologia da informação e de comunicação;

CONSIDERANDO a necessidade e importância de orientar membros, servidores, estagiários e terceirizados na implementação de medidas voltadas à gestão de segurança da informação do Ministério Público de São Paulo, com definição, análise e priorização de ações que correspondam aos objetivos e planejamento estratégico da instituição;

CONSIDERANDO a Lei n º 11.419/2006, que dispõe sobre a informatização do processo judicial, e a Portaria CNMP PRESI n° 153, de 07 de dezembro de 2017, que regulamenta a Política de Segurança Institucional do Conselho Nacional do Ministério Público;

CONSIDERANDO, por fim, as melhores práticas previstas na norma ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação, **EDITA** A SEGUINTE **RESOLUÇÃO**:

Art. 1º. Fica aprovada a Política de Segurança da Informação do Ministério Público de São Paulo, constante do Anexo I desta Resolução, cujo objetivo é assegurar que seus ativos, possuídos ou

custodiados, sejam utilizados e protegidos de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei.

Parágrafo único – No cumprimento desta Resolução, observar-se-ão a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e a Resolução nº 1.299/2021-PGJ, que instituiu a Política de Governança de Privacidade e Proteção de Dados Pessoais, no âmbito do Ministério Público de São Paulo, assim como os termos e definições constantes do Anexo II desta Resolução.

Art. 2º. Eventuais omissões serão decididas pelo Procurador-Geral de Justiça, após a oitiva do Comitê de Segurança Institucional.

Art. 3º. Esta resolução entra em vigor na data de sua publicação.

São Paulo, 20 de setembro de 2022.

MÁRIO LUIZ SARRUBBO
Procurador-Geral de Justiça

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1º. A política de segurança da informação tem por objetivo prover orientação, direção e apoio para a segurança da informação, de acordo com a legislação aplicável, dentre elas:
I - a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);
II - a Resolução 1.299/2021-PGJ, que instituiu a Política de Governança de Privacidade e Proteção de Dados Pessoais;
III - a Norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para controles de segurança da informação).

Art. 2º. A política de segurança de informação é destinada aos membros, servidores, estagiários e terceirizados que exercem atividade no Ministério Público de São Paulo.

Art. 3º. São diretrizes da política de segurança da informação:

I - assegurar que toda informação coletada, gerada, adquirida, utilizada, em trânsito e armazenada, própria, pessoal ou custodiada, por meio de tecnologias, procedimentos, pessoas e ambientes do Ministério Público de São Paulo, seja tratada como parte do seu patrimônio e protegida quanto aos aspectos de confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais, privacidade e conformidade legal;

II – assegurar a sua aplicação aos ambientes, sistemas, pessoas e processos do Ministério Público de São Paulo, tanto no meio digital, quanto nos meios analógicos de processamento, comunicação e armazenamento de informações;

III - estabelecer medidas de segurança pelo valor do ativo e em função dos riscos de impacto nas atividades e nos objetivos institucionais do Ministério Público de São Paulo, visando à proteção de dados pessoais, à privacidade e à conformidade legal, considerando o balanceamento de aspectos como tecnologias, austeridade nos gastos, qualidade e velocidade;

IV - considerar o membro, servidor, estagiário ou terceirizado, registrado no inventário de ativos, como responsável pelos ativos de informação e pela liberação e cancelamento do acesso, classificação de segurança e medidas de proteção de informação e dados;

V - segregar a administração e a execução de funções conflitantes ou áreas de responsabilidade críticas, visando reduzir os riscos de mau uso, acidental ou deliberado, dos ativos do Ministério Público de São Paulo;

VI - liberar o acesso e uso de ativos por meio de credencial, pessoal e intransferível, qualificando o titular como responsável por todas as atividades desenvolvidas por meio dela, sendo pré-requisito o preenchimento do Termo de Responsabilidade e Sigilo – TRS;

VII - assegurar que o acesso e o uso dos ativos sejam controlados e limitados às atribuições necessárias para cumprimento das atividades de membros, servidores, estagiários e terceirizados autorizados, no estrito interesse do Ministério Público de São Paulo, mediante a devida autorização;

VIII - permitir somente o uso de ativos homologados e autorizados pelo Ministério Público de São Paulo, desde que sejam identificados de forma individual, inventariados e protegidos, bem como tenham responsável e documentação atualizada, riscos mapeados, capacidade, manutenção e contingência adequadas e a sua operação esteja de acordo com a Política de Segurança da Informação do Ministério Público de São Paulo, a legislação em vigor e eventuais normas regulamentares ou contratuais incidentes;

IX – proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular;

X – assegurar que toda a cadeia de suprimentos de tecnologia da informação baseada em provedores de serviços no ambiente de computação em nuvem seja avaliada por todos os aspectos da segurança, incluindo o cumprimento da legislação e regulamentação local e global, o gerenciamento de identidades, o monitoramento e auditorias regulares e as restrições de localização geográfica para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo Ministério Público de São Paulo;

XI - assegurar a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos de trabalho do Ministério Público de São Paulo, por intermédio de ações de administração de crise, prevenção e recuperação, estabelecendo uma estratégia de continuidade de negócio para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas;

XII - monitorar e auditar periodicamente o cumprimento da Política de Segurança da Informação, pelas áreas competentes, respeitando-se os princípios normativos;

XIII - assegurar que membros, servidores, estagiários e terceirizados sejam continuamente capacitados e conscientizados sobre os procedimentos de proteção e uso correto dos ativos do Ministério Público de São Paulo na realização de suas atividades;

XIV - notificar a área responsável pelo tratamento de incidentes, caso o membro, servidor, estagiário ou terceirizado identifique qualquer quebra ou fragilidade na segurança da informação, enviando um e-mail para ctic@mpsp.mp.br;

XV – recomendar que diretrizes, normas e procedimentos da Política de Segurança da Informação sejam definidos, aprovados, publicados e comunicados aos membros, servidores, estagiários, e terceiros, observando, ainda, as diretrizes da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e da Resolução n° 1.299/2021-PGJ, que instituiu a Política de Governança de Privacidade e Proteção de Dados Pessoais.

Art. 4º. Cada espécie normativa da Política de Segurança da Informação deve ser revista em intervalos planejados, não superiores a 02 (dois) anos, a partir de sua data de publicação, ou em razão das seguintes hipóteses:

I - edição ou alteração de lei ou regulamento;

II - mudança estratégica da instituição;

III - expiração da data de validade do documento;

IV - mudança de tecnologia na organização;

V – necessidade em razão da coleta de resultados das análises de risco.

Art. 5º. Compete ao Centro de Tecnologia da Informação, ao Comitê de Apoio à Governança de Privacidade e Proteção de Dados Pessoais ou ao Comitê de Segurança Institucional as propostas de manutenção e atualização, o monitoramento periódico das normas e a complementação pelos demais instrumentos que compõem a Política de Segurança da Informação do Ministério Público de São Paulo.

Art. 6º. Compete ao Procurador-Geral de Justiça a aprovação das alterações das normas que compõem a Política de Segurança da Informação, após a manifestação do Centro de Tecnologia da Informação, do Comitê de Apoio à Governança de Privacidade e Proteção de Dados Pessoais e do Comitê de Segurança Institucional.

ANEXO II

TERMOS E DEFINIÇÕES

1. REFERÊNCIAS LEGAIS E NORMATIVAS

1. Constituição da República
2. Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente)
3. Lei nº 12.527/2011 (regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências)
4. Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)
5. Decreto nº 10.046/2019 (dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados)
6. ABNT NBR 16167:2013 (Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação)
7. ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para controles de segurança da informação)
8. ABNT NBR ISO 55000:2014 (Gestão de ativos - Visão geral, princípios e terminologia)
9. Recomendação nº 13/2009 do CNMP (dispõe sobre a implantação de Plano de Segurança Institucional nas áreas da segurança da informação, segurança de recursos humanos, segurança

de materiais, segurança de áreas e instalações: (https://www.cnmp.mp.br/portal/atos-e-normas-busca/norma/246)

10. Resolução nº 156/2016 do CNMP (institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, e dá outras providências: - https://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf).

11. Resolução nº 1.299/2021-PGJ (institui a Política de Governança de Privacidade e Proteção de Dados Pessoais).

12. Recomendações do MPSP na área de segurança institucional (http://www.mpsp.mp.br/portal/page/portal/Criminal/Recomendacoes/Seguran%C3%A7a_Aplicativos.pdf)

2. GLOSSÁRIO

Adware: qualquer forma de código ou programa de computador executado de forma automática e que exibe uma grande quantidade de anúncios, sem a prévia permissão do usuário.

Agentes de tratamento: o controlador e o operador (Lei nº 13.709/2018).

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Lei nº 13.709/2018).

Ataques do tipo DoS ou DDoS (Deny of Service ou Distributed Deny of Service): ataque de negação de serviços ou ataque distribuído de negação de serviços consistente na tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores, o que, de forma geral, não visa a invasão dos sistemas informáticos, mas sim a imposição de uma sobrecarga de uso (processamento ou número de acessos), indisponibilizando-os ou os tornando mais lentos.

Ativo: item, algo ou entidade que tem valor real ou potencial para uma organização (ref. ABNT NBR ISO 55000).

Ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso.

Atributos biográficos: dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios (Decreto nº 10.046/2019).

Atributos biométricos: características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar (Decreto n° 10.046/2019).

Atributos genéticos: características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas (Decreto nº 10.046/2019).

Bot: um tipo de ameaça digital (código ou programa de computador), cuja denominação advém do fato de funcionar de forma similar a um robô, podendo ser programado para realizar tarefas específicas ou para obter o total controle sobre o computador alvo.

Botnet: uma rede do tipo botnet é composta por um conjunto de computadores ou dispositivos conectados à internet, cada um executando um ou mais bots, que pode ser utilizada para a execução de ataques do tipo DoS/DDoS, para o furto de dados, para o envio de spams ou ainda para comprometer (com um vírus, por exemplo) o dispositivo alvo ao qual o invasor pretende atingir.

Classificação da informação: ação de definição do nível de sigilo da informação, a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização (Lei nº 13.709/2018, Resolução nº 1.299/2021-PGJ - Institui a Política de Governança de Privacidade e Proteção de Dados Pessoais e NBR27002:2013).

Computador zumbi: termo empregado para classificar um computador comprometido por alguma ameaça digital (bot, por exemplo) e utilizado para envio de spam e/ou ataques a sites, sem que o proprietário do computador tenha consciência de tal fato.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Lei nº 13.709/2018 e Resolução nº 1.299/2021-PGJ - Institui a Política de Governança de Privacidade e Proteção de Dados Pessoais).

Cracker / Hacker: de forma genérica, hackers são indivíduos que criam e/ou modificam softwares e hardwares ou dispositivos de um ambiente computacional, seja desenvolvendo funcionalidades novas ou adaptando as já existentes; cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de TI, de forma ilegal ou sem ética.

Credencial (ou conta de acesso): permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos, e cuja forma pode ser física (como um crachá) ou lógica (como a identificação de usuário e senha).

Criticidade: nível de crise (ou impacto) que pode advir da divulgação ou uso indevido da informação (Lei nº 13.709/2018, Resolução nº 1.299/2021-PGJ - Institui a Política de Governança de Privacidade e Proteção de Dados Pessoais e NBR16167:2013).

Custodiante da informação ou custodiante: usuários, grupos de trabalho ou áreas delegadas pelo proprietário do ativo de informação para cuidar da manutenção e guarda do ativo de informação no dia a dia, que geralmente não fazem parte do grupo de acesso e, portanto, não estão autorizados a acessar a informação (Lei nº 13.709/2018, Resolução nº 1.299/2021-PGJ - Institui a Política de Governança de Privacidade e Proteção de Dados Pessoais e NBR16167:2013).

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Lei nº 13.709/2018).

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2018).

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Lei nº 13.709/2018).

Dados cadastrais: informações identificadoras perante os cadastros de órgãos públicos, tais como os atributos biográficos, o número de inscrição no Cadastro de Pessoas Físicas – CPF, o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ, o Número de Identificação Social – NIS, o número de inscrição no Programa de Integração Social – PIS, o número de inscrição no Programa de Formação do Patrimônio do Servidor Público – Pasep, o número do Título de Eleitor, a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE e outros dados públicos relativos à pessoa jurídica ou à empresa individual (Decreto nº 10.046/2019).

Dados de crianças e adolescentes: informação relacionada à criança de até 12 anos de idade incompletos e adolescente entre 12 e 18 anos de idade (Lei nº 8.069/1990).

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (Lei nº 13.709/2018).

Grupo de acesso: pessoas, grupos de trabalho ou áreas autorizadas a terem acesso à determinada informação (Lei nº 13.709/2018 e NBR16167:2013).

Hoax (farsa): mensagem que tenta convencer o leitor de sua veracidade por um embuste ou farsa e depois tenta convencê-lo a realizar uma ação específica, cuja disseminação depende do envio deliberado da mensagem à outras vítimas em potencial, que também fazem o mesmo.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Lei nº 12.527/2018).

Informação de natureza pública: bem público, tangível ou intangível, com forma de expressão gráfica, sonora ou iconográfica, que consiste num patrimônio cultural de uso comum da sociedade e de propriedade das entidades/instituições públicas da administração centralizada, das autarquias e das fundações públicas, que pode ser produzida pela administração pública ou, simplesmente, estar em poder dela, para que esteja disponível ao interesse público ou coletivo da sociedade.

Keylogger: software que rastreia ou registra as teclas pressionadas em um teclado, geralmente de forma encoberta, para que a pessoa usando o teclado não esteja ciente de que suas ações estão sendo monitoradas. Isso geralmente é feito por pessoas mal-intencionadas para coletar informações, incluindo mensagens instantâneas, textos e endereços de e-mail, senhas, números de cartões de crédito e contas bancárias, endereços e outros dados privados.

Mapa de responsabilidades: documento contendo as funções, atribuições e responsabilidades de cada componente (integrante, grupo, comissão, departamento, diretoria, instituição etc.) de um projeto ou iniciativa, a fim de evitar dúvidas e conflitos entre os membros de cada equipe.

Nível de classificação: categoria a ser definida para cada informação ou classe de informação, que estabelece a sua sensibilidade em termos de preservação de sua confidencialidade, integridade e disponibilidade (NBR16167:2013).

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Lei nº 13.709/2018).

Phishing: forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, o que pode ocorrer de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros.

Proprietário do ativo de informação (ou responsável): parte interessada do Ministério Público de São Paulo, indivíduo legalmente instituído por sua posição ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Proteção de dados pessoais: tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Lei nº 13.709/2018).

Proxy anônimo: ferramenta que se esforça para fazer atividades na Internet sem vestígios, acessando a internet a favor do usuário ou protegendo as informações pessoais, ao ocultar a informação de identificação do computador de origem.

Rede de bots ou botnet: forma curta de "rede de robôs", é uma rede de computadores pirateados controlada remotamente por um hacker, que pode usá-la para enviar spam e lançar ataques de negação de serviço (DoS) e pode alugar a rede para outros cibercriminosos, inclusive a partir de um único computador em um botnet, pode-se automaticamente enviar milhares de mensagens de spam por dia.

Relatório de impacto à proteção de dados pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Lei nº 13.709/2018).

Rótulo: identificação física ou eletrônica da classificação atribuída à informação.

Segurança da informação: implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware (ref. NBR 27002:2013).

Screenlogger: tipo de ameaça digital capaz de capturar imagens/conteúdo das telas de computadores/dispositivos móveis, bem como de informar o posicionamento do cursor do mouse; e, quando utilizado em conjunto com um keylogger, pode ser usado para transmitir ao invasor as senhas e outras informações privadas do computador/usuário afetados.

Sigilo: grau de sigilo necessário para informação (Lei nº13.709/2018 e NBR16167:2013).

Smart card: cartão de plástico que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional de plástico com um chip de computador embutido.

Spam: mensagem eletrônica indesejada, geralmente não solicitada, enviada por mala-direta, para vários destinatários que não pediram para recebê-lo. Dentre os tipos de spam, estão o spam por e-mail, spam por mensagens instantâneas, spam por mecanismos de pesquisa da Web, spam em blogs e spam por mensagens em telefones celulares. O spam pode conter publicidade legítima, publicidade enganosa e mensagens de phishing que tentam defraudar os destinatários para obter informações pessoais e financeiras. As mensagens não são consideradas spam caso o usuário tenha feito a solicitação para recebê-las.

Spyware: tipo específico de código malicioso, programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Lei nº 13.709/2018).

Token: dispositivo físico gerador aleatório de código para uso como forma de autenticação.

Publicado em: DOE, Poder Executivo – Seção I, São Paulo, 132 (191), Quarta-feira, 21 de Setembro de 2022 p.61-62.