DEFENSORIA PÚBLICA
do Estado do Maranhão

ATO Nº 060 – DPGE, DE 30 DE SETEMBRO DE 2025

Institui a Política de Segurança da Informação (PSI) no âmbito da Defensoria Pública do Estado do Maranhão (DPE-MA).

O **DEFENSOR PÚBLICO-GERAL DO ESTADO DO MARANHÃO**, no uso da atribuição que lhe é conferida pelo artigo 17, VI da Lei Complementar Estadual nº 19, de 11 de janeiro de 1994 e pelo art. 97-A da Lei Complementar Federal nº 80, de 12 de janeiro de 1994.

CONSIDERANDO a norma ISO/IEC 27002:2013, traduzida pela Associação Brasileira de Normas Técnicas, estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação em instituições de qualquer esfera;

CONSIDERANDO as boas práticas de acesso e segurança à informação imprescindíveis à defesa da sociedade ou do Estado, previstas na Lei n.º 12.527/2011 - Lei de Acesso à Informação, com procedimentos a serem observados por todos os órgãos autônomos que compõem a estrutura do Estado;

CONSIDERANDO a necessidade de estabelecer políticas, diretrizes e procedimentos de segurança da informação, tendo em vista a imprescindibilidade de fornecer um ambiente tecnológico com níveis aceitáveis de controle e confiabilidade, para disponibilizar as informações necessárias aos processos de trabalho desta Defensoria com garantias de integridade, de disponibilidade, de confidencialidade, de autenticidade e de legalidade;

CONSIDERANDO a importância dos ativos de informação e a necessidade de regular a concessão de acessos aos sistemas informatizados e à rede de computadores; o uso da Internet e seus recursos; bem como o controle, monitoramento e auditoria de segurança da informação no âmbito desta Defensoria;

CONSIDERANDO a Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), que dispõe sobre o 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;

RESOLVE:

Art. 1º. Instituir a Política de Segurança da Informação (PSI) no âmbito da Defensoria Pública do Estado do Maranhão (DPE-MA), nos termos desta Resolução.

Art. 2º. A Política de Segurança da Informação é um conjunto de diretrizes a serem seguidas por todos(as) os(as) colaboradores(as), defensores(as), terceirizados(as), parceiros(as) e todos(as) que utilizam recursos computacionais da Defensoria Pública do Estado do Maranhão, dentro ou fora das suas instalações.

Art. 3º. A Defensoria Pública do Estado do Maranhão monitora e supervisiona todos os ambientes físicos e lógicos de sua propriedade ou sob seu controle, sem haver a necessidade de prévio consentimento ou notificação de terceiros(as), podendo manter registros do produto do monitoramento.

CAPÍTULO I
DOS OBJETIVOS

Art. 4º. A Política de Segurança da Informação tem por objetivo controlar o acesso à infraestrutura de comunicação e armazenamento de dados, evitando que os recursos computacionais da Defensoria Pública do Estado do Maranhão sejam utilizados em desrespeito às leis, às normas, aos costumes e à dignidade da pessoa humana, protegendo o ambiente computacional, rede corporativa e os ativos de informação contra ameaças e invasões advindas de acessos maliciosos, garantindo a integridade, a autenticidade, a confidencialidade e a disponibilidade das informações.

Art. 5º. Esta política deve ser interpretada de forma restritiva dentro do princípio da aplicação do menor privilégio possível, ou seja, no contexto de uso de informações e recursos de TIC,

tudo o que não tiver expressamente permitido só deve ser realizado após prévia autorização do Comitê de Segurança da Informação da Defensoria Pública do estado do Maranhão, devendo ser levada em consideração a análise de risco e a necessidade estratégica à época da solicitação.

Art. 6º. Esta política abrange todos(as) os(as) usuários(as) que possuam acesso à rede da Defensoria Pública do Estado do Maranhão, sejam integrantes da instituição, prestadores(as) de serviço, visitantes ou qualquer outra categoria.

Parágrafo único. Todos(as) os(as) usuários(as), internos e externos, com acesso a informações institucionais (de qualquer classificação) e a ambientes controlados da Defensoria Pública devem estar cientes do Termo de Compromisso e seguir esta política, operando dentro dos limites definidos.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 7º. Para efeitos desta Política, considera-se:

I - **Rede da Defensoria Pública**: Abrange todos os ativos, sistemas, diretórios e Intranet disponibilizados aos(às) usuários(as) da Defensoria Pública do Estado do Maranhão, conforme o perfil de acesso definido.

II - **Software:** São todos os programas homologados e disponibilizados pela equipe de TI para o exercício das funções, incluindo softwares instalados nos computadores e acessíveis via web.

III - **Homologação:** Verificação, pela equipe de TI, da compatibilidade técnica do software e dos aplicativos em relação ao parque tecnológico. Confirmação, pelo(a) usuário(a) final do sistema, do adequado funcionamento das funcionalidades previstas na implantação ou na atualização de versão do mesmo.

IV - **Ambiente Lógico**: Ambiente controlado, eletrônico, onde circulam e são armazenadas informações, softwares e sistemas.

V - **Ambiente físico**: Dependências físicas que integram a Defensoria Pública do Estado do Maranhão.

VI - **Usuários(as):** Defensores(as), servidores(as), residentes, estagiários(as), cedidos(as), terceirizados(as), prestadores(as) de serviço e quaisquer outros colaboradores(as) com acesso aos ambientes físicos e lógicos das instalações da Defensoria Pública do Estado do Maranhão.

VII - **Equipamentos Computacionais**: São todos os equipamentos disponibilizados ou aos quais os(as) usuários(as) tenham acesso na Defensoria Pública, incluindo, mas não se limitando a desktops, notebooks, smartphones corporativos, impressoras, equipamentos de videoconferência e digitalizadores.

VIII - **Informações institucionais**: Qualquer informação não disponível ao público externo ou reservada: dados, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, negociações, estudos, documentos e outros papéis de qualquer natureza (físicos ou em formato eletrônico), arquivos em qualquer meio, software e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Defensoria Pública em decorrência do desempenho de suas atividades.

IX - **Empresa:** Pessoa jurídica que mantenha contrato de prestação de serviço ou tenha celebrado instrumento similar com a Defensoria Pública.

X - **Visitante**: Qualquer pessoa que não mantenha vínculo formal com a Defensoria Pública, todo aquele que não se enquadre na definição de usuário(a).

CAPÍTULO III
DA PROPRIEDADE DAS INFORMAÇÕES E DOS SOFTWARES

Art. 8º. Todos os ativos físicos (hardware), lógicos (software) e informacionais da Defensoria Pública do Estado do Maranhão devem estar devidamente inventariados, identificados e revisados periodicamente.

Art. 9º. As informações processadas ou armazenadas pela Defensoria Pública são de sua propriedade, ou estão sob sua custódia legal, devendo ser utilizadas estritamente para fins institucionais e em conformidade com a legislação vigente.

§1º. O uso de software proprietário deve estar em conformidade com as licenças de uso corporativo, sendo proibida a utilização de software não autorizado.

Art. 10º. Os softwares desenvolvidos por terceiros(as) ou internamente, bem como todos os direitos relativos às invenções e inovações tecnológicas, elaboradas e/ou desenvolvidas (ou em desenvolvimento) pelos(as) usuários(as), durante a vigência da relação de trabalho, emprego ou contrato, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais, pertencem à Defensoria Pública, sendo vedada a cópia ou a disponibilização, por qualquer meio (eletrônico ou físico), para ambiente externo à Instituição.

Art. 11º. A disponibilização de softwares desenvolvidos pela instituição e suas atualizações se restringe aos termos de cooperação técnicas assinados entre a Defensoria Pública e outras instituições durante período de vigência do mesmo.

Art. 12º. Toda a estrutura mantida pela Defensoria Pública, composta pela rede, telefonia, correio eletrônico, internet e outros meios de comunicação são instrumentos de trabalho de sua propriedade, que a mesma disponibiliza aos(às) usuários(as), a fim de tornar suas tarefas mais eficientes. Da mesma forma, todos os documentos, estejam em formato impresso ou eletrônico, ou que circulem por esses meios, devem obedecer à política de classificação e aos controles de informação, conforme descrito na Seção 6 (Classificação da Informação) desta Política, de acordo com a criticidade das informações neles contidas.

Art. 13º. É proibido o uso desses documentos fora da Defensoria Pública, cujo objetivo não seja atender, exclusivamente, aos interesses da Instituição; ainda assim, sua retirada ou envio somente poderá ser efetuado com autorização dos(as) gestores(as) da área demandante.

Parágrafo único. A retirada ou o envio de informações para qualquer outra finalidade constitui violação desta Política.

§1º. Sua transmissão, via correio eletrônico ou outro meio, deverá ser feita seguindo as regras de segurança e confidencialidade constantes nesta Política.

§2º. Os documentos alterados fora da Instituição devem ter seus arquivos, manuais ou na rede, atualizados imediatamente.

CAPÍTULO IV
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 14º. A classificação de informações diz respeito à definição dos níveis de proteção que cada informação deve receber. Essa prática foi desenvolvida com o objetivo de reduzir vazamentos e acessos indevidos a dados importantes.

Art. 15º. O ato de classificar leva em consideração alguns requisitos do dado em questão, como valor, sensibilidade, requisitos legais e criticidade de cada arquivo para a Instituição. Por exemplo: arquivos que detalham as questões financeiras devem receber um nível de proteção maior do que a lista de colaboradores(as) designados para uma atividade específica.

Art. 16º. A classificação de informações faz parte das exigências feitas pela ISO 27001, norma que tem como objetivo a adoção de hábitos e processos que diminuam os riscos inerentes à segurança da informação.

Parágrafo único. As informações que transitam pela Defensoria Pública do Estado do Maranhão são, para fins desta Política, classificadas em quatro padrões distintos:

I - **Públicas:** Informações destinadas à disseminação fora da Defensoria Pública. Possuem caráter informativo geral e não são restritas aos(às) colaboradores(as) da Instituição, podendo ser divulgadas a todos(as), sem que isso provoque impactos nos negócios desta Instituição;

II - **Internas:** São aquelas destinadas ao uso dentro da Defensoria Pública. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a Defensoria Pública ou seus(suas) assistidos(as) e colaboradores(as). Essas informações não exigem proteções especiais, salvo aquelas entendidas como mínimas, para impedir a divulgação externa não intencional;

III - **Confidenciais:** Informações confidenciais, cuja exposição fora do ambiente da Defensoria Pública pode acarretar perdas financeiras, de imagem etc., sendo necessário, além do controle de acesso, a garantia de integridade, pois são informações importantes para as atividades da Instituição;

IV - **Restritas:** Informações altamente restritas, cujo acesso não autorizado, mesmo por membros da própria organização, é capaz de trazer sérios danos a atividade da Defensoria Pública. Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações confidenciais e, por isso, devem receber um grau de proteção ainda mais elevado. Só devem ter acesso às informações restritas as pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado;

Art. 17º. Em função desta categorização, é possível, no envio de informações sensíveis, a utilização de ferramentas que auxiliam na classificação de arquivos e mensagens, conforme sua criticidade, como soluções simples, baseadas em metadados, até plataformas corporativas mais complexas (por exemplo, Google Workspace), que devem ser consideradas sempre que a informação for disponibilizada ou encaminhada a terceiros(as).

Art. 18. A classificação da informação deve ser realizada pelo próprio setor que a produz ou detém, sendo indicada de forma clara em todos os documentos, mídias e sistemas que a contenham, utilizando marcadores visuais (como etiquetas, cabeçalhos e rodapés) ou metadados, e deve ser aplicada a todos os ativos de informação, incluindo:

I - **Documentos:** físicos e eletrônicos (e-mails, planilhas, apresentações, etc.).

II - **Mídias:** pendrives, discos rígidos, CDs, DVDs, etc.

III - **Sistemas:** aplicativos, bancos de dados, plataformas online, etc.

Parágrafo único. Todos os dispositivos que armazenam informações classificadas como confidenciais ou restritas devem ser protegidos por criptografia apropriada.

CAPÍTULO V
DA RESPONSABILIDADE

Art. 19. Compete ao Comitê de Segurança da Informação **(CSI):**

I - Definir a PSI e as políticas acessórias e garantir sua implementação e atualização;

II - Alocar os recursos tecnológicos necessários para a segurança da informação;

III - Assegurar a conformidade com as leis e as regulamentações de proteção de dados e segurança da informação.

Art. 20. Compete à Supervisão de Informática:

I - Implementar e gerenciar a Gestão de Segurança da Informação de TI, incluindo políticas, procedimentos, normas e controles de segurança, tendo como base esta Política e demais documentos acessórios;

II - Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

III - Monitorar os sistemas e as redes em busca de vulnerabilidades e incidentes de segurança;

IV - Apoiar o CSI em suas deliberações;

V - Promover a cultura de segurança da informação em todos os níveis da organização;

VI - Implementar medidas de segurança, técnicas e administrativas, para proteger os ativos de informação;

VII - Gerenciar a resposta a incidentes de segurança da informação;

VIII - Elaborar relatórios e indicadores de desempenho de segurança da informação;

IX - Realizar a gestão de riscos e incidentes de segurança da informação relacionada a dados pessoais.

Art. 21. Compete aos Supervisores(as) e Coordenadores(as):

I – Os(as) responsáveis por cada departamento ou área da Instituição, sejam supervisores(as) ou outros(as) profissionais com atribuição de gerir equipes e recursos de TI do respectivo setor, devem garantir que suas equipes tenham ciência e cumpram a PSI e as demais normas de segurança da informação;

II - Identificar e reportar incidentes de segurança da informação;

III - Colaborar na implementação de medidas de segurança;

IV - Assegurar que os acessos aos sistemas e às informações estejam de acordo com o princípio do mínimo privilégio;

V - Divulgar treinamentos e ações de conscientização sobre proteção de dados.

Art. 22. Compete aos Usuários(as):

I - Conhecer e cumprir a PSI e as demais normas de segurança da informação;

II - Proteger as informações sob sua responsabilidade contra acesso não autorizado, uso indevido e divulgação;

III - Utilizar os recursos computacionais de forma ética e responsável;

IV - Participar de treinamentos e ações de conscientização sobre segurança da informação;

V - Encaminhar quaisquer dúvidas ou pedidos de esclarecimento sobre a PSI, suas normas e procedimentos, à Supervisão de Informática ou, quando pertinente, ao CSI;

VI - Comunicar à Supervisão de Informática, através do e-mail suinfo@ma.def.br, qualquer evento que viole esta Política ou que represente, ainda que potencialmente, risco à segurança das informações ou dos recursos computacionais da Defensoria Pública do Estado do Maranhão;

VII - Ter ciência integral das disposições da PSI, bem como das demais normas e procedimentos de segurança, assumindo a responsabilidade pelo seu cumprimento.

CAPÍTULO VI
DOS PROCEDIMENTOS

Art. 23. As práticas de proteção da informação envolvem a definição de um conjunto de procedimentos, realizados de maneira sincronizada, para blindar os ativos virtuais e físicos relacionados à informação, independentemente de como eles são editados, compartilhados (enviados e recebidos), processados ou arquivados.

Art. 24. A Defensoria Pública do Estado do Maranhão utiliza, em sua plataforma, softwares e sistemas desenvolvidos internamente e adquiridos de terceiros(as).

Art. 25. Quando da admissão ou transferência de um(a) servidor(a) para outro setor, seus acessos aos sistemas e à rede serão automaticamente direcionados e restritos, em conformidade com o perfil de lotação. A liberação de acesso será analisada pelos setores envolvidos na solicitação do sistema, sendo passíveis de limites às funcionalidades do sistema, garantindo a restrição de acesso às informações críticas. Após as devidas aprovações, a área envolvida executará a liberação do acesso no respectivo sistema.

Art. 26. Em caso de necessidade de acessos diferenciados ou de utilização de softwares adicionais, o(a) profissional deverá contatar o suporte de TI, pelo sistema de Service Desk, disponível no endereço: https://suporte.ma.def.br, solicitando os acessos necessários.

Art. 27. Somente a SUINFO está autorizada a efetuar a instalação de softwares nas estações de trabalho.

Art. 28. O acesso aos computadores através da ferramenta de controle remoto deve ser utilizado apenas para suporte das equipes de atendimento ao usuário da SUINFO.

Parágrafo único. Para solicitação de suporte remoto em equipamentos funcionais, o(a) usuário(a) deverá entrar em contato somente através dos meios oficiais.

Art. 29. É terminantemente proibida a solicitação de suporte remoto diretamente ao contato pessoal da equipe responsável. Essa medida visa impedir que sejam feitas solicitações de suporte a técnicos(as) que já não estão mais a serviço da Defensoria Pública. O usuário deverá informar o nº ID do equipamento e aprovar o acesso.

Art. 30. Para garantir um ambiente digital seguro para todos(as), o acesso à rede Wi-Fi (onde existir) é segregado por SSID diferentes:

I - **WIFIDPEMA:** é liberado aos(às) usuários(as) da Defensoria Pública do Estado do Maranhão, mediante autenticação com login e senha.

II – **DPELIVRE:** para os(as) assistidos(as) e visitantes, com autenticação através de login único (SSO) de redes sociais ou voucher disponibilizado conforme evento.

Parágrafo único. Ao acessar e utilizar a rede Wi-Fi da Defensoria Pública, o(a) usuário(a) ou visitante concorda em cumprir a política de segurança da informação da Instituição.

Art. 31. A Defensoria Pública do Estado do Maranhão poderá disponibilizar acesso ao ambiente interno por meio de conexão remota segura, com uma credencial de usuário(a) autorizado(a).

Art. 32. Somente os(as) servidores(as) e os(as) defensores(as) que, eventualmente, tenham necessidade de utilizar a rede interna deverão solicitar a disponibilização de acesso, informando o nome do(a) usuário(a) que terá acesso ao recurso e qual aplicação o funcionário acessará.

Parágrafo único. A solicitação será feita no sistema de Service Desk, disponível no endereço: https://suporte.ma.def.br, e será analisada pela Supervisão de Informática.

Art. 33. A Defensoria Pública, pela natureza de suas operações, deve manter ambientes isolados para a manutenção de suas operações, por onde transitam informações sobre operações, posições e estratégias que só podem ser do conhecimento das áreas responsáveis pelo seu processamento. É terminantemente proibida a disponibilização indevida de tais informações ou a permissão de acesso ao ambiente segregado por pessoa não autorizada.

§ 1. As áreas que mantêm acesso controlado aos seus ambientes são:

I - Data center;

II - Salas técnicas.

§ 2º. O acesso de visitantes, inclusive ex-servidores(as), ao ambiente operacional da Defensoria Pública só poderá ocorrer com o acompanhamento de servidores(as) autorizados(as), sendo vedada a circulação de terceiros sem autorização específica para isso.

Art. 34. Somente técnicos(as) vinculados(as) à Supervisão de Informática (SUINFO) estão autorizados(as) a realizar a instalação de equipamentos na rede de comunicação da Defensoria Pública.

Art. 35. É proibida a instalação de quaisquer equipamentos que não sejam homologados pela ANATEL, em conformidade com a legislação vigente e com as normas técnicas de segurança e qualidade.

Art. 36. É proibida a instalação, na rede de comunicação da Defensoria Pública, de equipamentos que não sejam fornecidos ou expressamente autorizados pela própria instituição, tais como:

I - Roteadores;

II - Repetidores;

III - Adaptadores Wireless USB;

IV - Switches;

V - Hubs.

§ 1º. A vedação da instalação desses equipamentos visa garantir a integridade, a disponibilidade e a confidencialidade das informações trafegadas na rede institucional, conforme os princípios da Política de Segurança da Informação (PSI) da Defensoria Pública.

§ 2º. Em casos excepcionais, a instalação de quaisquer dos equipamentos listados deve ser previamente analisada e expressamente autorizada pela SUINFO, mediante justificativa formalizada e alinhada à Política de Segurança da Informação da instituição.

Art. 37. As práticas de proteção da informação envolvem a definição de um conjunto de procedimentos, realizados de maneira sincronizada, para blindar os ativos virtuais e físicos relacionados à informação, independentemente de como eles são editados, compartilhados (enviados e recebidos), processados ou arquivados.

Art. 38. O acesso à internet é permitido a todos(as) os(as) usuários(as), com o objetivo de facilitar suas tarefas. Assim como qualquer outro material de trabalho, as páginas da internet também devem ser usadas somente para fins profissionais.

Art. 39. O acesso à internet é permitido a todos(as) os(as) assistidos(as) e visitantes, com o objetivo de facilitar o acesso a aplicativos e sistemas estritamente necessários durante sua permanência dentro da instituição.

§ 1º. Para uma utilização eficiente e produtiva, algumas regras devem ser obedecidas:

I - É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, violência, atividades de hacker e quaisquer outras atividades ilegais.

II- Fica proibido, também, o download de programas não autorizados ou sem revisão e prévia aprovação da SUINFO.

§ 2º. Estes exemplos não esgotam a lista de sites proibidos, portanto, quaisquer dúvidas devem ser levadas ao conhecimento da Supervisão de Informática (SUINFO), pelo e-mail: suinfo@ma.def.br.

§ 3º. Todos os acessos são registrados para fins de auditoria quando solicitado visando identificar falsos positivos e novos sites indevidos ainda não bloqueados.

§ 4º. Aliada a essa funcionalidade, há o controle de acesso aos sites não permitidos, relatados anteriormente, impedindo que os mesmos sejam acessados. Quaisquer atividades que contrariem as regras de acesso à internet ficarão sujeitas à penalidade.

Art. 40. Quando um(a) usuário(a) observar a necessidade de acessar um determinado site que está previamente bloqueado, para fins profissionais, é possível solicitar o acesso a ele abrindo um chamado no sistema de Service Desk, via link https://suporte.ma.def.br/, informando através do formulário específico o endereço do site, a justificativa para acessá-lo e o período em que precisa acessá-lo.

§ 1º. A SUINFO analisará a solicitação, verificando, junto ao(à) gestor(a) imediato(a), a real necessidade de acesso ao site.

§ 2º. Em caso de aprovação, também serão definidas as seguintes ações:

I - Site liberado para todos(as) os(as) usuários(as) da Instituição?

II - Site liberado para todos(as) os(as) usuários(as) do setor?

III - Site liberado apenas para o(a) solicitante?

§ 3º. Em casos de acessos temporários, o(a) usuário(a) deverá informar por quanto tempo o acesso deverá ser liberado. Essas informações são essenciais para a adequada administração dos acessos temporários aos sites bloqueados.

Art. 41. É proibida a prática de roteamento do acesso à internet disponibilizado pela Defensoria Pública, por meio de quaisquer dispositivos ou configurações que permitam o compartilhamento não autorizado da conexão de rede institucional.

§ 1º. Os dispositivos de identificação e senhas protegem a identidade do(a) usuário(a), evitando e prevenindo que uma pessoa se faça passar por outra perante a Defensoria Pública e/ou terceiros(as).

§ 2º. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

§ 3º. A utilização indevida das informações obtidas em razão de acesso aos sistemas, atendimentos entre outras formas de coleta de informações, poderá se enquadrar nos tipos penais

previstos nos artigos 319 (prevaricação), 320 (condescendência criminosa), 321 (advocacia administrativa), 325 (violação do sigilo funcional) e 326 (violação do sigilo de proposta de concorrência pública) do Código Penal.

Art. 42. Algumas regras referentes à composição e uso de senhas de acesso, com o objetivo de assegurar sua confidencialidade:

I - A senha deve ser trocada imediatamente após o primeiro acesso.

II - Depois disso, a troca será efetuada mediante solicitação automática do sistema ou por solicitação do(a) próprio(a) usuário(a);

III - A senha deverá ser composta por, pelo menos, oito (08) caracteres, mesclando letras maiúsculas e minúsculas, números e caracteres especiais (ex: #, @, $, &). É importante ressaltar que, quanto maior a senha, maior a dificuldade em decifrá-la;

IV - Não é recomendado o uso de senhas com nomes próprios, números de telefone, nome da conta no sistema, datas de aniversário, caracteres idênticos repetidos (ex:11111, aaaaa) ou sequenciais (ex: abcdef, 12345);

V - Evite reutilizar senhas antigas;

§ 1º. Não se deve guardar anotações de senhas em blocos de anotações, post-it nos monitores, embaixo dos teclados, anotado no calendário, embaixo do aparelho telefônico, agendas ou qualquer local de fácil acesso;

§ 2º. Cada usuário(a) é inteiramente responsável pelo uso de sua conta de acesso à rede, suas senhas e outros tipos de autorização, que são de uso individual e intransferível, e não podem ser compartilhados com colegas de trabalho ou terceiros(as). Nessa situação, o(a) membro(a), servidor(a) ou eventual colaborador(a) será responsável por ações indevidas que venham a ser efetuadas a partir de sua conta de acesso à rede ou sistemas, caso alguém obtenha acesso à sua conta devido a não utilização de senhas seguras;

§ 3º. A periodicidade máxima para troca automática das senhas é 180 (cento e oitenta) dias, não podendo ser repetidas as 3 (três) últimas senhas.

Art. 43. Após a criação de uma nova conta, as credenciais serão enviadas para os(as) usuários(as), seguindo as regras abaixo:

I - O link para definição da senha de acesso à rede, sistemas e e-mail corporativo deverá ser enviado para o e-mail informado no formulário disponibilizado no sistema para criação de usuário.

Parágrafo único. Em caso de esquecimento da senha de acesso à rede ou sistemas, deverá ser encaminhada solicitação de reset de senha para o e-mail: suinfo@ma.def.br e o link para redefinição de senha será encaminhada para o e-mail pessoal ou corporativo cadastrado.

Art. 44. Quando um(a) usuário(a) é desligado(a) da Defensoria Pública, perde imediatamente o direito de acesso aos equipamentos, serviços e sistemas e ao serviço de e-mail corporativo. Este procedimento é iniciado imediatamente pela Supervisão/Unidade responsável pelo gerenciamento do vínculo, por meio de solicitação através de formulário disponibilizado no sistema de Service Desk, via link https://suporte.ma.def.br/, que revogará o acesso de autenticação do(a) usuário(a).

§ 1º. Em casos que o desligamento não amigável, a solicitação de desligamento deverá ser comunicada de forma imediata pelo setor/unidade responsável pela gerência do vinculado a ser desligado, através do e-mail: suinfo@ma.def.br.

§ 2º. No caso de transferências internas de um(a) servidor(a) para outro setor, os direitos de acesso originais são retirados na data prevista da transferência. Os novos acessos são liberados automaticamente com o novo cadastro de lotação do(a) usuário(a), bem como aos demais sistemas e ambientes da rede referentes às atividades da nova área.

§ 3º. No caso de afastamento por férias, licença ou qualquer outro motivo que não seja o desligamento, o setor/unidade responsável pelo controle de vínculo do(a) usuário(a) com a instituição deverá comunicar a SUINFO através do sistema de Service Desk, via link https://suporte.ma.def.br/.

§ 4º. Os trabalhos desenvolvidos ou elaborados pelo(a) servidor(a) pertencem exclusivamente à Defensoria Pública, não cabendo ao servidor(a) o direito de retirá-los ou copiá-los quando de seu desligamento, não sendo permitida a gravação de arquivos em qualquer mídia, sem a devida autorização de seu superior imediato.

§ 5º. A responsabilidade pela conservação de cada equipamento é do membro, servidor(a) e/ou eventual colaborador(a) que o utiliza diariamente.

§ 6º. Ao se ausentar da mesa, mesmo que por um curto período, o computador deverá ser bloqueado usando as teclas CTRL + ALT + DEL e selecionar a opção bloquear ou pressionar as teclas □ + L para bloquear a estação.

Art. 45. Não é permitido instalar softwares sem o conhecimento da SUINFO. A instalação de softwares que não fazem parte do catálogo oficial de softwares homologados para uso da instituição, deverá ser encaminhada a SUINFO através do sistema de Service Desk, disponível no endereço: https://suporte.ma.def.br, para que possa ser devidamente analisada pela área, observando as regras internas e sem prejudicar a segurança da instituição como um todo além da legalidade para utilização em ambiente corporativo.

Art. 46. A manutenção física dos equipamentos (adição, remoção e substituição de hardware) é de responsabilidade da SUINFO, sendo proibido aos(às) membros(as), servidores(as) e demais colaboradores(as) da Defensoria Pública de outras áreas a execução dessas atividades.

§ 1º. Os equipamentos disponibilizados pela Defensoria Pública aos(às) seus(suas) membros(as), servidores(as) e demais colaboradores(as) são para uso profissional, relacionado às atividades da instituição.

§ 2º. É vedada a utilização de equipamentos pertencente a Defensoria Pública para meios ilícitos, como, por exemplo, envio de material sexualmente explícito ou implícito; conteúdo ofensivo, preconceituoso ou discriminatório, apologia à violência ou atos terroristas, apologia às drogas, violação de direitos autorais, acessos não autorizados a equipamentos de terceiros(as), qualquer tipo de atividade relacionada a fraude, entre outros.

§ 3º. O(a) membro(a), servidor(a) e demais colaboradores(as) da Defensoria Pública devem prezar pela individualidade de suas credenciais de acesso, não podendo, em hipótese alguma, compartilhar seu login e senha de acesso aos sistemas e sites corporativos.

Art. 47. Não são permitidas alterações de configurações no hardware, no sistema operacional e de padrões dos aplicativos disponibilizados nos equipamentos cedidos pela Defensoria Pública para trabalho externo, estando o(a) membro(a), servidor(a) ou eventual colaborador(a) infrator(a) sujeito(a) às sanções disciplinares da Política de Segurança da Informação, bem como, responsabilizado(a) pelos danos causados aos referidos equipamentos ou ações legais em decorrência da utilização/consumo de conteúdo ilegal, softwares piratas ou não registrados pela Defensoria Pública.

§ 1º. O equipamento cedido ao(à) servidor(a) ou eventual colaborador(a) deve ser utilizado para a execução das atividades relacionadas a Defensoria Pública.

§ 2º. As informações armazenadas nos equipamentos cedidos pela instituição não devem, em hipótese alguma, ser distribuídas, copiadas, compartilhadas ou cedidas para quem quer que seja, em qualquer meio, seja impresso, magnético ou transcrito sem justificativa válida de interesse da Instituição;

§ 3º. É de responsabilidade do(a) membro(a), servidor(a) ou colaborador(a) a salvaguarda das informações armazenadas nos equipamentos portáteis, uma vez que o disco rígido do equipamento é passível a falhas;

§ 4º. Em caso de falha em qualquer dispositivo do equipamento em questão, o(a) usuário(a) não deverá procurar assistência técnica ou fazer qualquer substituição de componentes (disco rígido, baterias, carregadores, antenas etc.) sem a autorização prévia da SUINFO;

§ 5º. Em caso de roubo, furto, perda total ou parcial do equipamento recebido, o(a) usuário(a) deverá comunicar imediatamente seu superior, bem como à SUINFO, e providenciar o registro do respectivo boletim de ocorrência (BO) junto à autoridade policial;

§ 6º. Todas as regras citadas acima valem para notebooks, celulares, smartphones, etc., fornecidos pela Defensoria Pública aos(às) seus(suas) membros(as), servidores(as) e eventuais colaboradores(as);

§ 7º. Quando em viagem, e sempre que possível, os computadores portáteis devem ser levados como bagagem de mão, tendo em vista critérios de segurança da informação;

Art. 48. O uso de dispositivos portáteis de uso pessoal está restrito exclusivamente à rede Wi-Fi DPELIVRE e suas limitações, sendo vedado o acesso desses equipamentos à rede corporativa. Essa medida é necessária para mitigar riscos à segurança da informação e à integridade dos sistemas institucionais.

Art. 49. Dispositivos pessoais, em geral, não seguem os mesmos padrões de segurança aplicados aos equipamentos corporativos, como atualizações regulares, proteção antivírus e políticas de criptografia. Isso os torna mais vulneráveis a infecções por malware, ataques de phishing e outras ameaças cibernéticas, podendo servir como porta de entrada para agentes maliciosos na rede interna.

Além disso, a perda ou roubo desses dispositivos pode resultar em exposição ou vazamento de dados sensíveis.

Art. 50. A frequência e periodicidade de realização dos backups devem ser definidas conforme a necessidade do negócio, a criticidade da informação para a continuidade das operações, requisitos de segurança e auditoria.

Art. 51. Os backups devem ser armazenados em local distante do data center principal que ofereça proteções contra alta temperatura, umidade e acessos não autorizados.

Art. 52. Semestralmente, a equipe da SUINFO deverá realizar testes de Recuperação de Dados por amostragem, com o objetivo de atestar a integridade e disponibilidade dos dados armazenados.

§ 1º. A recuperação deve ser integral de pelo menos um servidor/sistema escolhido aleatoriamente, e deve ser planejada e documentada para fins de auditorias futuras.

§ 2º. As falhas referentes a problemas no processo de backup e restore de informações devem ser registradas e reportadas.

§ 3º. Os registros de falhas devem ser avaliados para assegurar que estas foram satisfatoriamente resolvidas e que as medidas corretivas aplicadas pós-falhas foram documentadas no chamado.

§ 4º. A restauração das cópias de backup deve ser realizada através da abertura de chamado com a aprovação do(a) proprietário(a) da informação.

§ 5º. Para casos relacionados a incidentes com servidores(as), fica a critério da SUINFO avaliar a necessidade de recuperação, a fim de restabelecer o ambiente o mais rápido possível.

CAPÍTULO VII
DAS NOTIFICAÇÕES DE SEGURANÇA

Art. 53. Todos os sistemas operacionais, sistemas de aplicativos e equipamentos de redes devem ser devidamente configurados para que gerem logs de eventos, segurança e auditoria.

§ 1º. Todos os equipamentos devem gerar seus logs em um servidor centralizado, para evitar o risco de adulteração dos logs, e para que seja possível realizar a correlação dos eventos.

Art. 54. O acesso direto a banco de dados em ambientes produtivos, por parte de servidores(as) ou eventuais colaboradores(as) que não fazem parte da SUINFO não é permitido, tanto para consulta, quanto para edição de dados.

Art. 55. Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes.

Art. 56. É responsabilidade dos(as) usuários(as) notificar a SUINFO, através do e-mail suinfo@ma.def.br, sempre que se deparar com uma atitude que considere abusiva ou de risco à segurança da informação, para que sejam tomadas as devidas ações, minimizando os impactos da ocorrência.

Art. 57. Nos casos de incidentes de segurança que envolvam dados pessoais, será observado o disposto na Ato nº 25 DPGE/MA – Política de Proteção de Dados, devendo a SUINFO comunicar o fato ao(à) Encarregado(a) de Proteção de Dados, endereçando e-mail ou processo administrativo próprio.

CAPÍTULO VIII
DAS SANÇÕES

Art. 58. As violações, mesmo que por mera omissão ou tentativa não consumada, desta Política, bem como das demais normas e dos procedimentos de segurança, estarão sujeitas a penalidades, em conformidade com a legislação regente, a depender da gravidade do fato, do cargo e do tipo de vínculo do(a) colaborador(a) com a Instituição.

§ 1. A aplicação de sanções será realizada conforme a análise dos órgãos competentes, devendo-se considerar a gravidade da infração, o efeito alcançado, a recorrência e as hipóteses previstas na legislação aplicável e suas atualizações.

Art. 59. No caso de terceiros(as) contratados(as) ou prestadores(as) de serviço, o(a) gestor(a) responsável deverá analisar a ocorrência e deliberar sobre a efetivação das sanções, conforme os termos previstos em contrato e nas normas vigentes. As pessoas jurídicas contratadas podem ser responsabilizadas pelos atos dos(as) referidos(as) colaboradores(as) funcionários(as), prepostos(as), representantes, subcontratados(as) ou qualquer outra pessoa que esteja a serviço da contratada.

§ 1º. Para o caso de violações que impliquem atividades ilícitas ou que possam acarretar danos à Defensoria Pública, além da penalidade imposta, o infrator será responsabilizado pelos prejuízos, cabendo a tomada das medidas judiciais pertinentes.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 60. Os casos omissos serão avaliados pelo CSI, para posterior deliberação.

Art. 61. As diretrizes, estabelecidas nesta Política, em seus anexos e nas demais normas e procedimentos de segurança, não se esgotam, em razão da contínua evolução tecnológica e do constante surgimento de novas ameaças, não constituindo rol exaustivo, sendo obrigação do usuário da informação da Defensoria Pública adotar, sempre que possível, outras medidas de segurança, além das aqui previstas, com o objetivo de garantir a proteção às informações da Instituição.

Art. 62. Este Ato entra em vigor na data de sua publicação.

Gabinete da Defensoria Pública-Geral do Estado, em São Luís/MA, 30 de setembro de 2025.

GABRIEL SANTANA FURTADO SOARES
Defensor Público-Geral do Estado do Maranhão