Aprovado pela Deliberação nº 33/2021 - CSPGE, de 20 de maio de 2021 (D.O.E nº 10.941, 24/05/2021)

Institui a Política de Segurança da Informação da Procuradoria-Geral do Estado - PGE.

CAPÍTULO I

DO OBJETIVO E DA ABRANGÊNCIA

Art. 1º A Política de Segurança da Informação é o conjunto de princípios e diretrizes que têm a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da Procuradoria-Geral do Estado do Paraná - PGE.

Art. 2º Estão submetidos à Política de Segurança da Informação todos os procuradores, servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que, por força de quaisquer instrumentos, exerçam atividades no âmbito da PGE, bem como qualquer pessoa que venha a ter acesso aos ativos de informação da PGE.

Parágrafo único. A Política de Segurança da Informação aplica-se aos contratos, convênios, acordos e outros instrumentos congêneres em que a da PGE esteja envolvida.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º São princípios que regem a Política de Segurança da Informação da PGE:

I - respeito e promoção dos direitos e garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

II - proteção dos dados, informações e conhecimentos produzidos na PGE;

III - orientação à gestão de riscos e à gestão da segurança da informação;

IV - prevenção e tratamento de incidentes de segurança da informação;

V - garantia do sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas;

VI - exigência de *necessidade de conhecer* para o acesso à informação sigilosa, nos termos da legislação;

VII - sensibilização e conscientização dos usuários.

CAPÍTULO III

DAS DEFINIÇÕES

Art. 4º Para os efeitos desta Política de Segurança da Informação são estabelecidas as seguintes definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

IV - contas de Serviço: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.);

V - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

VI - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

VII - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser biométrica; física, como crachá, cartão e selo; ou lógica, como identificação de usuário e senha;

VIII - exclusão de acesso: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso;

IX - gestão de riscos de segurança da informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

X - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

XI - perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XIII - incidente de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XIV - termo de uso e responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XV - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XVI - usuário: procuradores, servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que exerçam atividades no âmbito da Procuradoria-Geral do Estado do Paraná que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da PGE, formalizada por meio da assinatura do termo de uso e responsabilidade.

CAPÍTULO IV

DAS DIRETRIZES

SEÇÃO I

Das Diretrizes Gerais

Art. 5º São diretrizes gerais desta Política de Segurança da Informação:

I - toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela PGE deve ser protegida, esteja ela em meio físico ou digital;

II - os recursos de tecnologia da informação disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da PGE;

III - a identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso a informações e recursos de tecnologia da informação na PGE;

IV - o acesso e o uso da informação e dos recursos de tecnologia da informação devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário;

V - qualquer outra forma de acesso ou uso, para além dos descrito dos incisos II e IV deste artigo, necessita de prévia autorização do gestor do ativo de

informação e da chefia imediata do usuário, observando-se a legislação em vigor;

VI - a conveniência, para que o nível adequado de proteção para a informação seja estabelecido, de que as informações, existentes e futuras, tenham seu grau de sigilo estabelecido;

VII - a definição de, no mínimo, um responsável para receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como identificar tendências tecnológicas e comportamentais;

VIII - a definição de medidas, regras e procedimentos para assegurar que as funções ou atividades críticas da PGE possam ser mantidas ou recuperadas, após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações;

IX - o levantamento regular dos aspectos legais de segurança aos quais as atividades da PGE estão submetidas e o seu cumprimento, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

X - o estabelecimento de controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da PGE e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo-se a entrada e saída de visitantes, pessoal interno, equipamentos e mídias;

XI - a capacitação contínua de procuradores, servidores e estagiários para o desenvolvimento de competências em Segurança da Informação;

XII - as informações, os sistemas e os métodos criados por procuradores servidores e estagiários da PGE, no exercício de suas funções, são patrimônios intelectuais do Estado do Paraná, não cabendo a seus criadores qualquer forma de direito autoral, ressalvado o disposto na Lei nº 10.973/2004;

XIII - as medidas de proteção da informação e as despesas na aplicação de controles devem ser planejadas e compatibilizadas com o valor do ativo a ser protegido;

XIV - os requisitos de segurança da informação devem estar explicitamente citados nos termos de compromisso celebrados entre a PGE e terceiros nos casos pertinentes;

XV - o acesso às informações, sistemas e instalações depende da apresentação de credencial ou termo de uso e responsabilidade, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

XVI - quando do afastamento, mudança de responsabilidade, atribuições ou lotações dos usuários dentro da instituição, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

XVII - quando da admissão ou do desligamento de usuário, cabe ao Grupo de Recursos Humanos Setorial comunicar tal fato imediatamente ao setor de tecnologia da informação, para adoção das medidas cabíveis relativas à concessão ou à exclusão dos direitos de acesso e de uso dos ativos de informação.

§ 1º O ativo produzido em e-mail institucional e na rede corporativa pelo usuário desligado deverá ser mantido pela PGE por, no mínimo, 30 (trinta) dias, garantindo-se o reconhecimento e o esclarecimento da propriedade do acervo.

§ 2º O usuário terá acesso apenas aos sistemas e informações que realmente necessitar para a execução de sua atividade laboral.

§ 3º Todos os usuários devem preencher e autenticar termo de uso e responsabilidade.

§ 4º A solicitação de acesso a sistema ou a informação deverá ser formulada pela chefia imediata do usuário interessado.

§ 5º Cabe ao chefe do setor responsável pelo sistema ou pela informação a concessão de autorização de acesso ao usuário interessado.

§ 6º As dúvidas e conflitos em torno da concessão de autorização de acesso serão resolvidas pela Diretoria-Geral.

SEÇÃO II

Das Diretrizes Específicas

Art. 6º São diretrizes específicas para a criação e administração de contas de acesso:

I - a criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário;

II - o usuário que não exerce funções de administração da rede local somente terá disponibilizada uma única conta institucional de acesso à rede, pessoal e intransferível;

III - a conta de acesso no perfil de administrador será utilizada somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

IV - O usuário deve assumir a responsabilidade pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de termo de uso e responsabilidade;

V - A criação de contas de serviço exige regras específicas.

Art. 7º São diretrizes específicas para controle de acesso à rede corporativa de computadores:

I - concessão de credenciais de acesso à rede corporativa de computadores somente após a data de contratação ou de entrada em exercício do usuário;

II - exclusão de credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário;

III - registro dos acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário pelo período mínimo de 60 (sessenta) meses;

IV - implementação, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, *tokens*, *smart cards*, a fim de autenticar a identidade do usuário da rede;

V - utilização de mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores;

VI - manutenção, na rede corporativa, de mecanismos que permitam identificar e rastrear os endereços de origem e destino internos e externos, bem como os serviços utilizados;

VII - utilização da legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro;

VIII - gravação do acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada.

Art. 8º São diretrizes específicas para controle de acesso aos ativos de informação:

I - utilização de ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada;

II - respeito ao princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

III - utilização de ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;

IV - registro de eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

V - criação de mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 9º São diretrizes específicas para uso da internet:

I - o acesso à Internet no âmbito da PGE deve ser realizado com a finalidade exclusiva de executar as atividades de interesse público e àquelas desempenhadas pelo órgão, observando sempre a moralidade administrativa;

II - o setor de tecnologia da informação monitorará os acessos à internet, recursos e sistemas de informação dentro das dependências da PGE e bloqueará sites que tenham conteúdo suspeito e perigoso para a execução dos objetivos, missão e visão da Instituição;

III - caso o usuário observe que algum site suspeito ou perigoso esteja com acesso liberado, deverá informar imediatamente ao setor de tecnologia da informação.

Art. 10. São vedados:

I - a instalação de softwares não homologados ou licenciados pelo setor de tecnologia da informação;

II - o acesso ou a tentativa de acesso a recurso tecnológico do qual não seja detentor de autorização, em especial àqueles que contenham conteúdo considerado ofensivo, ilegal ou impróprio;

III - a utilização dos recursos tecnológicos da PGE para fins estranhos às atividades desta instituição;

IV - a prática de quaisquer atos tendentes a tornar indisponível qualquer recurso tecnológico sem autorização;

V - o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente de rede da PGE.

Art. 11. São diretrizes específicas para uso do correio eletrônico:

I - é obrigatório o uso do correio eletrônico corporativo como meio de envio e recebimento de informações inerentes às atividades institucionais da PGE, vedada a sua utilização para fins particulares;

II - comprova-se a distribuição de mensagens e informações corporativas e institucionais por qualquer meio que demonstre o envio para o endereço eletrônico do destinatário;

III - o acesso diário à caixa de mensagens eletrônicas corporativa é responsabilidade exclusiva do usuário;

IV - o setor de tecnologia da informação deve adotar medidas para bloquear o acesso, pela rede da PGE, aos servidores de correios eletrônicos comerciais quando identificado o mau uso.

Art. 12. São diretrizes específicas para o tratamento de incidentes:

I - as falhas em sistemas de informação devem ser registradas imediatamente via abertura de chamado pela intranet endereçado ao setor de tecnologia da informação;

II - caso o sistema não esteja acessível e outro computador próximo não estiver disponível - ou seja, uma falha geral - o chamado poderá ser aberto por telefone, cabendo à área de atendimento ao usuário o registro, posteriormente, no sistema de chamados;

III - a Coordenadoria de Gestão Estratégica e Tecnologia da Informação é encarregada de coordenar a equipe de tratamento e resposta a incidentes de segurança e de acompanhar as investigações e as avaliações dos danos decorrentes destes incidentes.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

SEÇÃO I

Das Competências

Art. 13. No âmbito da Política de Segurança da Informação da PGE, caberá à Coordenadoria de Gestão Estratégica e Tecnologia da Informação – CGTI:

I - promover a cultura de segurança da informação;

II - definir regras específicas sobre criação de contas de serviço;

III - assessorar a implementação das ações de segurança da informação;

IV - propor recursos necessários às ações de segurança da informação;

V- definir, no mínimo, um responsável para receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança;

VI - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança;

VII - coordenar a equipe de tratamento e resposta a incidentes em redes computacionais;

VIII - definir medidas, regras e procedimentos para assegurar que as funções ou atividades críticas da PGE possam ser mantidas ou recuperadas, após falha ou interrupção na operação normal dos sistemas;

IX - levantar regularmente os aspectos legais de segurança aos quais as atividades da PGE estão submetidas;

X - realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação;

XI - propor normas e procedimentos internos relativos à segurança da informação, em conformidade com as legislações existentes sobre o tema;

XII - levar à Diretoria-Geral os casos omissos e excepcionais.

Parágrafo único. As competências previstas neste artigo poderão ser atribuídas no todo ou em parte a colegiado específico responsável pela gestão e governança na área de tecnologia da informação no âmbito da PGE, conforme dispuser seu ato de instituição.

SEÇÃO II

Das Responsabilidades

Art. 14. São deveres dos usuários dos sistemas e dos ativos de informação da PGE:

I - cumprir fielmente esta Política, as normas complementares, as orientações específicas e os procedimentos de segurança da informação da PGE;

II - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação ou, ainda, do Gestor de Segurança da Informação da PGE;

III - assinar termo de sigilo e/ou termo de uso e responsabilidade que formalizará a ciência e o aceite desta Política de Segurança da Informação, bem como estabelecerá responsabilidade pessoal por seu descumprimento;

IV - sempre que se ausentar da estação de trabalho, o usuário deve bloquear o acesso, seja por meio do encerramento da sessão virtual, seja por meio do desligamento da máquina;

V - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela PGE;

VI - comunicar, imediatamente, ao Gestor de Segurança da Informação qualquer descumprimento ou violação desta Política ou de seus documentos complementares da qual vier a ter conhecimento.

Art. 15. O logon e a senha de rede e de sistemas de informações são a identidade do usuário na PGE.

§ 1º Para cadastrar sua senha, o usuário deve se identificar por meio de documento de identidade ou equivalente e preencher termo de uso e responsabilidade.

§ 2º A identidade do usuário é pessoal e intransferível, sendo o usuário o responsável exclusivo pela proteção da sua identidade.

Art. 16. O usuário é responsável por todos os atos praticados com suas identificações, dentre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital.

Art. 17. O usuário é responsável pela integridade do equipamento computacional que está operando.

Art. 18. O usuário responderá pela segurança dos ativos, dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

Art. 19. O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

Art. 20. A PGE poderá, a qualquer tempo, realizar o bloqueio de acesso e revogar credenciais de acesso concedidos a usuários em virtude do descumprimento desta Política de Segurança da Informação ou das normas e procedimentos específicos dela decorrentes.

Art. 21. O usuário que fizer uso de forma indevida ou não autorizada dos ativos de informação, bem como agir em desacordo com os termos desta Política, fica sujeito à aplicação das penalidades previstas nos estatutos funcionais de regência, garantidas a ampla defesa e o contraditório.

Art. 22. O descumprimento das disposições constantes nesta Política e nas normas complementares sobre segurança da informação será apurado em processo administrativo disciplinar, sem prejuízo das responsabilidades civil e penal.

CAPÍTULO VI

DA REVISÃO, COMPLEMENTAÇÃO E VIGÊNCIA

Art. 23. Esta Política de Segurança da Informação será revisada periodicamente, em intervalos não superiores a 2 (dois) anos, por iniciativa da Diretoria-Geral ou da Coordenadoria de Gestão Estratégica e Tecnologia da Informação.

Art. 24. A Diretoria-Geral, mediante portaria, aprovará modelo de termo de uso e responsabilidade e poderá aprovar:

I - norma específica para o acesso e a cessão de equipamentos;

II - norma específica para a autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação;

III - norma específica para o bloqueio e a exclusão de contas de acesso;

IV - norma específica para o uso de redes sem fio;

V - norma específica para o uso da Internet, do Correio Eletrônico, de Mensagens Instantâneas e armazenamento de arquivos;

VI - norma específica para definição de perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso;

VII - norma específica para o armazenamento, a requisição e a veiculação de imagem, vídeo ou áudio registrados em perímetros de segurança;

VIII - norma específica para movimentação de equipamentos de informática e procedimentos de sanitização no caso de baixa patrimonial ou transferência definitiva entre órgãos.

Parágrafo único. As competências previstas nos incisos I, II, III, IV, V e VIII poderão ser atribuídas no todo ou em parte a colegiado específico responsável pela gestão e governança na área de tecnologia da informação no âmbito da PGE, conforme dispuser seu ato de instituição.

Art. 25. Esta Política de Segurança da Informação entrará em vigor na data da sua publicação.