Política de Segurança da Informação

PODER JUDICIÁRIO
DO ESTADO DA BAHIA

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO
11/06/2025	1.0	Versão inicial

SUMÁRIO

CAPÍTULO I – DAS DISPOSIÇÕES GERAIS 3
CAPÍTULO II – DA ESTRUTURA NORMATIVA DE SEGURANÇA DA INFORMAÇÃO 3
CAPÍTULO III – Das diretrizes.....4
CAPÍTULO IV – Dos princípios 4
CAPÍTULO V – Dos papéis e responsabilidades 5
CAPÍTULO VI – Do tratamento da informação.....6
CAPÍTULO X – DA VIGÊNCIA 11

CAPÍTULO I – DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Política de Segurança da Informação do Tribunal de Justiça do Estado da Bahia, aqui denominada PSI, é uma declaração formal do compromisso da Alta Administração deste Tribunal com a proteção de dados e informações de sua propriedade ou sob sua guarda.

§ 1º Esta PSI norteará a implementação de medidas protetivas que deverão ser aplicadas a toda e qualquer informação ou dado, independente do meio que se encontre, para resguardar a imagem e objetivos institucionais deste Tribunal.

§ 2º Suas orientações devem ser lidas, entendidas, seguidas, cumpridas e divulgadas em todos os níveis hierárquicos e a todos que de alguma forma tenham interação com este Tribunal, para que seu patrimônio, a informação, tenha o grau de confidencialidade, integridade e autenticidade exigidos pela sociedade.

Art. 2º Para os fins do disposto nesta PSI, a Segurança da Informação abrange:

I. A segurança cibernética;

II. A defesa cibernética;

III. A segurança física;

IV. A proteção de dados organizacionais e pessoais;

V. As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no âmbito do TJBA.

CAPÍTULO II – DA ESTRUTURA NORMATIVA DE SEGURANÇA DA INFORMAÇÃO

Art. 3º A estrutura normativa da Segurança da Informação do TJBA é composta por documentos, alinhados em três níveis hierárquicos – Política ➔ Normas ➔ Procedimentos – e relacionados a seguir:

I. **Política de Segurança da Informação:** Define a estrutura, estabelece as diretrizes e define as responsabilidades referentes à Segurança da Informação. É documento público, sem restrições de acesso;

II. **Normas de Segurança da Informação:** Estabelecem obrigações e definem procedimentos a serem seguidos de acordo com as diretrizes da Política. As normas são departamentais ou setoriais. Os acessos são concedidos conforme necessidade de operação;

III. **Procedimentos de Segurança da Informação:** Definem as regras operacionais conforme o disposto nas Normas e na Política de Segurança, permitindo sua utilização nas atividades do TJBA.

Art. 4º As normas e os procedimentos são elaborados por cada órgão do Poder Judiciário do Estado da Bahia (esses documentos são específicos para o TJBA), de forma a atender às suas especificidades próprias, sempre de acordo com as diretrizes aqui definidas. A Política também.

CAPÍTULO III – DAS DIRETRIZES

Art. 5º A PSI alcançará todas as unidades do Tribunal de Justiça do Estado da Bahia, de acordo com as seguintes diretrizes:

I. Proteção do direito individual e coletivo das pessoas quanto à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição Federal e demais legislações pertinentes;

II. Gestão permanente da Segurança da Informação, provendo os recursos físicos, tecnológicos, humanos e ambientais adequados para a manutenção desta Política, racionalizando os custos e minimizando os riscos;

III. Cooperação entre as unidades do Tribunal de Justiça do Estado da Bahia, bem como entre os conveniados, contratados, demais órgãos e Poderes Públicos, promovendo o intercâmbio científico-tecnológico e de informações relativas a eventos de risco e a Segurança da Informação;

IV. Padronização de processos e soluções, assegurando a interoperabilidade entre os sistemas de informação;

V. Otimização da alocação de recursos e tecnologias nos vários níveis da segurança orgânica por meio da Gestão de Riscos de Segurança da Informação;

VI. Elaboração e implementação de programas de conscientização e capacitação que se fizerem necessários para a efetiva implantação desta PSI, com a fiel observância a seus dispositivos, normativos e demais procedimentos complementares;

VII. Adoção consistente e racionalizada de tecnologias de segurança da informação.

CAPÍTULO IV – DOS PRINCÍPIOS

Art. 6º As ações decorrentes desta PSI serão regidas pelos seguintes princípios:

I. **Autenticidade:** Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos;

II. **Celeridade:** As ações de Segurança da Informação devem oferecer respostas rápidas a incidentes e falhas de segurança;

III. **Confidencialidade:** Garantia de que a informação esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade devidamente autorizados;

IV. **Conhecimento:** Os usuários devem conhecer e respeitar esta PSI, normas internas e demais regulamentações sobre Segurança da Informação;

V. **Clareza:** As normas e procedimentos de Segurança da Informação devem ser precisas, concisas e de fácil entendimento;

VI. **Disponibilidade:** Garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, conforme acordado;

VII. **Ética:** Os direitos e interesses legítimos das partes envolvidas devem ser preservados, sem comprometimento da Segurança da Informação;

VIII. **Integridade:** Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino;

IX. **Privacidade:** Garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais;

X. **Responsabilidade:** Os donos da informação (quem gera a informação) tem a responsabilidade primária e final pela segurança dos dados utilizados e das informações geradas e pelo cumprimento de processos de segurança, que devem ser claramente definidos; (definir ativos e dono da informação)

XI. **Publicidade:** A publicidade de informações é preceito geral e o sigilo é exceção;

CAPÍTULO V – DOS PAPÉIS E RESPONSABILIDADES

Art. 7º Para efeito desta PSI, são estabelecidos os seguintes papéis e responsabilidades:

I. **De todos os magistrados, servidores e demais colaboradores do TJBA:** Conhecer, divulgar e seguir as regras definidas nesta Política de Segurança da Informação. Comunicar, nos canais devidos, quaisquer comportamentos, incidentes ou fatos que impactem na segurança da informação no TJBA;

II. **De todo gestor:** Ter postura exemplar em relação à Segurança da Informação e disseminar as boas práticas definidas pelo TJBA em todos os seus atos e em sua área de atuação, sendo de sua responsabilidade gerir os acessos dos magistrados, servidores e demais colaboradores do TJBA aos sistemas de informação.

III. **Do Comitê Gestor de Segurança da Informação - CGSI:** Contribuir para a constante evolução da Segurança da Informação na instituição, sem prejuízo no disposto na Resolução nº 14, de 31 de agosto de 2013, incluindo: as atribuições do CGSI estão definidas no decreto que o criou

a) Reunir-se, semestralmente ou quanto algum evento se justificar, para analisar temas relevantes sobre Segurança da Informação e sua aplicabilidade no TJBA;

b) Assessorar a implementação das ações de segurança da informação;

c) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

d) Participar da elaboração e revisão da PSI e das normas de segurança da informação;

e) Propor alterações à PSI às normas de segurança da informação;

f) Deliberar sobre normas internas de segurança da informação;

g) Estabelecer mecanismos de monitoramento da gestão da segurança da informação;

h) Comunicar, pelo menos semestralmente, à Alta Gestão do Tribunal os indicadores de gestão da segurança da informação;

i) Deliberar sobre as ações propostas pelo gestor de segurança da informação no parecer técnico sobre o relatório de avaliação de conformidade e riscos de

segurança da informação, encaminhando à alta administração para aprovação;

j) Propor investimentos e projetos em Segurança da Informação;

IV. **Da Secretaria de Tecnologia da Informação e Modernização – SETIM:** A SETIM deverá:

a) Assegurar o apoio técnico e operacional no planejamento estratégico da segurança institucional e de TI, para a implantação e manutenção das tecnologias empregadas no Tribunal;

b) Elaborar normativos técnicos complementares a este documento, e demais anexos, quanto ao quesito da Segurança da Informação;

c) Realizar anualmente uma análise de riscos de Segurança da Informação, submetendo ao CGSI um plano de ação para mitigação de riscos e vulnerabilidades;

d) Manter uma estrutura de tratamento e respostas a incidentes de Segurança da Informação – ETIR.

V. **Das Diretorias da SETIM:** Garantir que os sistemas e ambiente tecnológico utilizados pelos magistrados, servidores, demais colaboradores e usuários dos sistemas e equipamentos do TJBA forneçam proteção adequada às informações durante todo o seu ciclo de vida (criação, armazenamento, uso, transferência, arquivamento e descarte);

VI. **Dos gestores e fiscais dos contratos de prestação de serviço:** Manter registro, manutenção e eliminação, no sistema de controle de acesso, dos dados dos funcionários vinculados aos respectivos contratos;

VII. **Da Secretaria de Administração do Tribunal de Justiça do Estado da Bahia, em conjunto com o Gabinete de Segurança Institucional:** Garantir o apoio técnico e operacional no planejamento estratégico da segurança institucional.

CAPÍTULO VI – DO TRATAMENTO DA INFORMAÇÃO

Art.8º As informações geradas, coletadas, processadas, analisadas, compartilhadas, armazenadas, reutilizadas ou eliminadas em meio digital no TJBA devem ser protegidas por login e senha.

Art.9º As informações críticas devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente.

Art. 10º A gestão de acessos a informação deverá obedecer ao princípio de menor privilégio possível, podendo os usuários terem acesso a não mais do que as informações e recursos computacionais necessários para o pleno desenvolvimento de suas atividades administrativas.

§ 1º. As credenciais de acesso concedidas aos usuários são pessoais e intransferíveis, podendo seu uso ser auditado e monitorado, não devendo o usuário conceder suas credenciais a terceiros, sob quaisquer circunstâncias.

Art. 11º Toda informação que possa identificar uma pessoa, deve ser precedida de análise de impacto à privacidade, antes de ser divulgada, respeitando-se a finalidade e os princípios previstos na Lei 13.709/2018, na política de tratamento de dados pessoais e demais regulamentos internos do TJBA.

Art.12º As informações críticas que devem possuir métodos de controle de acesso rígido, de modo que somente pessoas autorizadas e acompanhadas possam ter acesso.

§ 1º. Todos os acessos devem ser registrados e as autorizações devem ter tempo determinado, o controle de acesso deve ser preferencialmente de forma eletrônica, através de biometria, cartões de acesso ou reconhecimento facial.

§ 2º. Todos os acessos deverão ter seu registro (log) armazenado conforme norma própria aprovada pelo CGSI.

VII - Da classificação da informação

Art. 13º Conforme o status da informação em seu ciclo de vida, elas deverão ser classificadas como:

a) Ultrassecreta – O mais alto grau de restrições. Esta classificação deverá ter aprovação pelos Magistrados;

b) Secreta – Informações restritas a acesso pessoal, como senhas, processos internos assim classificados, ou classificadas por outras legislações e normas internas. Podem ser os processos administrativos disciplinares e outros cobertos por segredo de justiça.

c) Reservada – Informações restritas a normas, procedimentos operacionais internos e outros documentos pertinentes exclusivamente a ações e processos internos de trabalho.

d) Pública - Classificam-se as informações de domínio público, sejam internos ou externos ao TJBA.

§ 1º. Uma norma de classificação da informação deverá ser elaborada, adequada a cada processo de trabalho do TJBA e aprovada pelo CGSI.

VIII - Da gestão de riscos e da gestão de incidentes

Art. 14º O processo de gestão de riscos de segurança da informação alinha-se à gestão de riscos da segurança institucional.

Art. 15º A gestão de incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

§ 1º. Os Magistrados, Servidores e demais colaboradores do TJBA são responsáveis por:

a) informar imediatamente à CGSI e a SETIM os incidentes com a segurança da informação de que tenham ciência ou suspeita;

b) colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação.

Art. 16º O Comitê Gestor de Segurança da Informação - CGSI, juntamente com a Secretaria de Tecnologia da Informação e Modernização - SETIM e sob sua responsabilidade, desenvolverá e implementará os processos e métodos necessários e suficientes para:

c) Realizar anualmente uma análise corporativa de riscos de segurança da informação;

d) Elaborar um plano de ação para tratamento de riscos, ameaças e vulnerabilidades identificadas para ser executado em cada área específica;

e) Viabilizar, que as áreas críticas e sensíveis do TJBA implementem mecanismos de gestão de riscos conforme a sua finalidade e foco;

IX - Do uso de recursos operacionais e de comunicações

Art. 17º Os recursos de informática disponibilizados pelo TJBA são fornecidos com o propósito único de garantir o desempenho das atividades de cada Magistrado, Membro, Servidores ou colaboradores, sendo vedado o uso desses recursos para:

a) constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica;

b) veicular opiniões político-partidárias, religiosas e quaisquer outras atividades que contrariem os objetivos institucionais;

c) atividades particulares.

Secção I – Do e-mail institucional

Art. 18º Entende-se por e-mail institucional a conta de e-mail criada com o domínio @tjba.jus.br, podendo ser das seguintes espécies:

a) Contas de e-mail institucional individual: para acesso individual e único atribuído a Magistrados, Servidores e colaboradores;

b) Contas de e-mail institucional compartilhadas: a fim de representar unidade administrativa ou judicial do PJBA, um sistema de informação, uma campanha de comunicação ou assemelhados.

§ 1º. Todos os servidores e magistrados ativos terão contas de e-mail institucional individual, sendo obrigatória sua utilização.

Art. 19º. O acesso ao conteúdo armazenado nas contas de e-mail é privativo de cada titular, vedado acesso de terceiros sem autorização expressa do titular da conta ou da Presidência do TJBA.

Parágrafo único. A Presidência do Tribunal de Justiça autorizará o acesso ao conteúdo da conta de e-mail individual nas seguintes situações:

I – apuração de faltas funcionais em procedimento administrativo formalmente constituído;

II – comprovado risco segurança da informação;

III – procedimento legal e;

IV – necessidade de continuidade de operações.

Art. 20º Compete à SETIM

I – implementar medidas para gerenciar o espaço de armazenamento das contas de e-mail;

II – alertar aos usuários quanto ao eventual mau funcionamento ou interrupção do serviço de e-mail;

III – comunicar oficialmente a chefia imediata quanto da eventual má utilização do e-mail por integrantes de sua equipe;

IV - monitorar a frequência de utilização das caixas compartilhadas visando inativação ou exclusão de caixas que não tenham leitura acompanhada;

V - suspender o acesso do usuário à conta de e-mail em caso de indícios de mau uso ou violação da confidencialidade, disponibilidade e autenticidade das informações ou credenciais de acesso, informando oficialmente a chefia imediata;

VI – bloquear o envio e a recepção de e-mails caracterizados como SPAM, sempre que tecnicamente viável.

Art. 21º Compete aos usuários de e-mail institucional:

I – utilizar as contas de e-mail exclusivamente para atividades laborais ou de interesse da Instituição;

II – não utilizar o e-mail institucional para enviar propaganda de qualquer natureza, exceto referente a eventos apoiados ou patrocinados pelo Poder Judiciário;

III – não utilizar o e-mail institucional para compras ou vendas pessoais, envio de correntes, boatos ou mensagens de procedência duvidosa etc.;

IV – não utilizar o e-mail institucional para encaminhamento de mensagens ofensivas a honra ou a dignidade das pessoas ou instituições, bem como para quaisquer atividades consideradas ilegais;

V – manter sua credencial de acesso protegida e para uso individual;

VI – não fornecer as listas de e-mails individuais ou de grupos do TJBA a terceiros;

VII – utilizar o campo CCO (Com Cópia Oculta) nos endereçamentos de e-mail que tenham lista ampla de destinatários;

VIII – Não utilizar o e-mail institucional para o envio de mensagens festivas ou comemorativas, exceto pela Coordenadoria de Comunicação da Presidência ou da Corregedoria.

IX – executar, no mínimo mensalmente, procedimentos de exclusão, arquivamento ou transferência de conteúdo para evitar o esgotamento das respectivas cotas de armazenamento.

X - Da auditoria e conformidade

Art. 22º O CGSI e a SETIM, deverão em conjunto com as áreas de controle interno e auditoria promover, em até um ano da publicação desta PSI, a incorporação de procedimentos de auditoria de riscos e conformidade para garantir a correta aplicação da PSI e suas normas.

XI - Do treinamento e conscientização

Art. 23º Com o objetivo de manter um processo de treinamento e conscientização em Segurança da informação, fica estabelecido que:

a) É de responsabilidade do Comitê Gestor de Segurança da Informação prover treinamento sobre Segurança da Informação a todos os Magistrados, Servidores e demais colaboradores, bem como realizar atividades pontuais para aumentar a conscientização com relação a esta PSI.

b) Essas atividades podem ser realizadas através de cursos on-line EAD, mensagens eletrônicas disparadas periodicamente, notícias e dicas de utilização disponibilizadas na intranet, eventos anuais de Segurança da Informação, entre outras atividades.

c) A não realização dos treinamentos obrigatórios definidos pelo TJBA poderá ocasionar no bloqueio dos acessos à rede e sistemas em caso de não participação por parte dos Magistrados, Servidores e demais colaboradores do TJBA.

XII - Das penalidades

Art. 24º. Os Magistrados, Servidores e demais colaboradores do TJBA que descumprirem esta Política de Segurança da Informação ou suas normas decorrentes, responderão em processo administrativo disciplinar, ficando sujeitos a devidas sanções.

Art. 25º. No caso de descumprimento desta Política de Segurança por prestadores de serviços sob contratos do Tribunal, a infração será classificada como possível motivo de quebra do Contrato de Prestação de Serviços, independentemente de medidas judiciais cabíveis nas esferas penal, cível e administrativa.

§ 1º. Em todos os casos, sempre será assegurado o contraditório e a ampla defesa.

XIII – Revisão

Art. 26º Esta PSI deverá ser revisada anualmente, por proposição do CGSI, ou quando algum fato ou evento a justificar.

XIV - Considerações finais

Art. 27º. Todas as áreas do TJBA, através de seus gestores, deverão adequar seus processos, procedimentos e ações à esta PSI.

Art. 28º Fica determinado o prazo de até 90 (noventa) dias para a SETIM e o CGSI atualizarem as normas e procedimentos decorrentes desta política, determinando sua classificação e publicação.

Art. 29º. Esta Política de Segurança da Informação entra em vigor a partir de sua publicação.

Art. 30º. Fica revogado o Decreto Judiciário Nº 474, de 16 de agosto de 2019, e seus anexos.

CAPÍTULO X – DA VIGÊNCIA

Art. 14º Esta Política entra em vigor na data de sua publicação, por tempo indeterminado.