Publicada no Diário da Justiça Eletrônico 87, em 6 de maio de 2022.

RESOLUÇÃO 773, DE 29 DE ABRIL DE 2022.

Dispõe sobre a Política de Segurança da Informação (PSI/STF).

O PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, no uso de suas atribuições, observado o art. 363, inc. I, do Regimento Interno do Supremo Tribunal Federal;

CONSIDERANDO que o Tribunal produz e recebe informações no exercício de suas competências constitucionais, legais e regulamentares, e que tais informações devem permanecer íntegras, disponíveis, com autenticidade garantida e eventual sigilo resguardado;

CONSIDERANDO que as referidas informações são armazenadas em diferentes suportes e veiculadas por diversas formas, estando sujeitas a vulnerabilidades como desastres naturais, acessos não autorizados, uso indevido, falhas de equipamentos, extravio e furto;

CONSIDERANDO o advento da Lei 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no art. 5º, inc. XXXIII, no art. 37, § 3º, inc. II, e no art. 216, § 2º, da Constituição Federal;

CONSIDERANDO o disposto no art. 13 da Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

CONSIDERANDO as boas práticas em segurança preconizadas pelas Normas Técnicas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011; 27014:2013 e 31.000:2009;

CONSIDERANDO a necessidade de implementar ações para garantir a adequada execução da Lei nº 13.709/2018 (LGPD), no que tange à segurança da informação;

CONSIDERANDO o Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal;

CONSIDERANDO o Anexo III da Resolução nº 638/2019, que instituiu a Política de Gestão de Riscos Corporativos do STF;

CONSIDERANDO que o Sistema de Governança do Supremo Tribunal Federal - SIGOV-STF, aprovado pela Resolução nº 755, de 13 de dezembro de 2021, prevê em seu art. 3º, que compõem a estrutura de governança do STF, as Instâncias Superiores de Governança; a Alta Administração; e as Instâncias de Apoio à Governança;

CONSIDERANDO que a Resolução que dispõe sobre o SIGOV, prevê no § 3º do art. 5º, que poderão ser criadas, na Política de Governança Organizacional ou

mediante normativo próprio, novas instâncias de apoio à governança com temáticas específicas;

CONSIDERANDO o Ato Regulamentar nº 25, de 29 de novembro de 2021, que altera dispositivos do Regulamento da Secretaria e cria a Assessoria de Segurança da Informação (ASI) e o Núcleo de Prevenção, Tratamento e Resposta a Incidentes em Segurança da Informação do Supremo Tribunal Federal (NPTRI);

CONSIDERANDO a Instrução Normativa nº 01 - DSIC/GSI/PR, de 27 de maio de 2020, que estabelece diretrizes para a elaboração de Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar GSI Nº 5, de 14 de agosto de 2009, que disciplina a criação de Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos da administração pública federal;

CONSIDERANDO a Resolução CNJ 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO o contido no Processo Administrativo Eletrônico nº 004814/2021,

R E S O L V E:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação do Supremo Tribunal Federal (PSI/STF).

Art. 2º Para os efeitos desta Resolução e de suas regulamentações, aplicar-se-á o glossário de termos de segurança da informação definido e publicado no Portal Corporativo da Secretaria de Tecnologia e Inovação. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~Art. 2º Para os efeitos desta Resolução e de suas regulamentações, aplicar-se-á o glossário de termos de segurança da informação definido e publicado no Portal Corporativo do STF.~~

Art. 3º São destinatários desta PSI e estão a ela submetidos todas as autoridades, servidores e quaisquer colaboradores do STF, que fazem uso ou tenham acesso aos ativos de informação e de processamento no âmbito do Tribunal.

Art. 4º A PSI/STF se alinha ao Sistema de Governança e às estratégias do STF, tendo como princípios norteadores:

I - garantia da integridade e da autenticidade das informações produzidas;

II - preservação da integridade e da autenticidade das informações recebidas;

III - confidencialidade das informações com necessidade de restrição de acesso, por meio de proteção adequada;

IV - garantia da disponibilidade das informações custodiadas;

V - transparência das informações públicas;

VI - gestão das ações de segurança da informação por meio de uma abordagem baseada em riscos.

Art. 5º As informações produzidas por autoridades, servidores e quaisquer colaboradores do STF, no exercício de suas atribuições, constituem patrimônio do Tribunal, não cabendo a seus criadores qualquer forma de direito autoral.

§ 1º Quando as informações forem produzidas por colaboradores do STF para uso exclusivo pelo Tribunal, deverá ser confeccionado instrumento próprio contendo as obrigações dos criadores, inclusive no que se refere à eventual confidencialidade das informações.

§ 2º É vedada a utilização das informações a que se refere o § 1º deste artigo pelos colaboradores do STF em projetos ou atividades diversas daquelas estabelecidas pelo Tribunal, salvo mediante autorização específica dos Ministros nos processos e documentos de sua competência, ou do Presidente, nos demais casos.

CAPÍTULO II
DAS DIRETRIZES E OBJETIVOS

Art. 6º A estrutura normativa referente à Segurança da Informação será estabelecida e organizada conforme as diretrizes definidas a seguir:

I - Nível Estratégico: PSI/STF, constituída por esta Resolução, a qual define as diretrizes fundamentais e os princípios basilares da área;

II - Nível Tático: normas complementares sobre segurança da informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~II - Nível Tático: normas complementares sobre segurança da informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI, a serem editadas pelo Tribunal, devendo abarcar, no mínimo, os seguintes temas:~~

~~a) Gestão de Ativos;~~

~~b) Controle de Acesso à Informação;~~

~~c) Gestão de Riscos em Segurança da Informação;~~

~~d) Gestão de Cópias de Segurança;~~

~~e) Plano de Continuidade de Serviços Essenciais de TI;~~

~~f) Gestão de Incidentes de Segurança da Informação;~~

~~g) Gestão de Vulnerabilidades e Padrões de Configuração Segura;~~

~~h) Gestão e Monitoramento de Registros de Atividade (*logs*);~~

~~i) Desenvolvimento Seguro de Sistemas;~~

~~j) Uso de Recursos Criptográficos;~~

~~k) Uso Aceitável de Recursos de TI;~~

~~l) Utilização da Computação em Nuvem;~~

~~m) Utilização do Trabalho Remoto;~~

III - Nível Operacional: procedimentos de segurança da informação que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto nas normas complementares, permitindo sua utilização nas atividades do órgão.

§ 1º Conforme a necessidade e conveniência do Tribunal, poderão ser criados normativos sobre outros temas.

§ 2º Os normativos deverão considerar as disposições contidas nas normas e padrões nacionais e internacionais de segurança da informação.

Art. 7º São objetivos da PSI do STF:

I - instituir estratégias, responsabilidades e competências, visando à estruturação da segurança da informação;

II - direcionar as ações necessárias à implementação e manutenção da segurança da informação;

III - definir as ações necessárias para evitar ou mitigar os efeitos de atos acidentais ou intencionais, internos ou externos, de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV - nortear os trabalhos de conscientização e de capacitação de pessoal em segurança da informação e em proteção de dados pessoais.

Parágrafo único. A segurança da informação abrange aspectos tecnológicos, humanos e os aspectos relacionados ao tratamento das informações, que acontece no âmbito de cada unidade do Tribunal.

Art. 8º O uso adequado dos recursos de tecnologia da informação e comunicação tem como objetivo garantir a continuidade da prestação jurisdicional e de serviços do STF.

§ 1º Os recursos de tecnologia da informação e comunicação, pertencentes ao Tribunal e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação e comunicação é passível de monitoramento e controle por parte do Tribunal.

CAPÍTULO III
DA ESTRUTURA DE GOVERNANÇA (NR)

(**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~CAPÍTULO III~~
~~DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E DA ESTRUTURA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO~~

Art. 9º O Comitê de Segurança da Informação (CSI/STF), instância temática de apoio à governança, possui natureza consultiva e deliberativa, sendo subordinado à Presidência do Tribunal e composto, no mínimo pelo:

I - Secretário-Geral da Presidência ou pessoa por ele indicada; (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~I - Gestor de Segurança da Informação;~~

II - Chefe de Gabinete da Presidência ou pessoa por ele indicada; (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~II - Secretário de Tecnologia da Informação;~~

III - Diretor-Geral ou pessoa por ele indicada; (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~III - Secretário de Segurança;~~

IV - responsável pela área de tecnologia da informação; (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~IV - Supervisor do Núcleo de Prevenção, Tratamento e Resposta a Incidentes em Segurança da Informação;~~

~~V - Assessor-Chefe da Assessoria de Projetos Judiciais.~~ (**Revogado pela Resolução nº 805, de 1º de agosto de 2023, publicada no DJe do dia 3 de agosto de 2023**)

VI - responsável pela segurança institucional; (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

VII - responsável pela área de segurança cibernética; (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

Art. 10. Compete ao CSI/STF:

I - estabelecer a direção estratégica para a segurança da informação, alinhando-a com os objetivos de negócio da organização. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~I - avaliar e propor estratégias a que se referem esta Política;~~

II - garantir que os riscos de segurança da informação sejam identificados, avaliados e tratados de forma adequada, incluindo a decisão sobre a aceitação de riscos

e alocação de recursos para a mitigação de ameaças. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~II - monitorar os riscos de segurança da informação, informando a alta administração sobre os riscos considerados críticos;~~

III - garantir que a segurança da informação receba o investimento necessário em termos de pessoal, tecnologia e orçamento, demandando recursos para manter os níveis de risco aceitáveis e aumentar a maturidade da segurança. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~III - demandar recursos para manter os riscos de segurança da informação em níveis que seus membros entendam aceitáveis;~~

IV - monitorar o desempenho da segurança da informação, acompanhando métricas e indicadores-chave para avaliar a eficácia das medidas de segurança, o nível de maturidade da organização e a aderência à PSI e às normas de segurança da informação incluindo a revisão periódica desta Política e planos de segurança. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~IV - monitorar a maturidade em segurança da informação e demandar recursos para aumentá-la, gradativamente;~~

V - supervisionar o cumprimento de leis e regulamentos relevantes de segurança da informação. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~V - manifestar-se sobre iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre segurança da informação, além de outras matérias que lhe sejam submetidas, submetendo à alta administração o que não estiver na alçada decisão de seus membros.~~

VI - aprovar estratégias, normas, procedimentos, planos ou processos relativos à segurança da informação que forem submetidos ao comitê, submetendo à Presidência as propostas que extrapolem sua alçada decisória. (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

§ 1º Cabe às unidades do Tribunal implementar e acompanhar a operacionalização de ações de segurança da informação nas respectivas áreas.

§ 2º O CSI/STF será coordenado pelo Secretário-Geral da Presidência ou por representante por ele designado, o qual assumirá o papel de Gestor de Segurança da Informação do STF. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~§ 2º O CSI/STF será coordenado pelo Gestor de Segurança da Informação.~~

~~Art. 11. Compete à Assessoria de Segurança da Informação (ASI), unidade vinculada ao Gabinete da Presidência:~~ (**Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~I – propor a elaboração e a revisão desta política, diretrizes, normas e procedimentos inerentes à segurança da informação, bem como analisar periodicamente sua efetividade, nos termos do art. 6º desta PSI;~~

~~II - propor ações visando à fiscalização da aplicação das normas e da política de segurança da informação;~~

~~III - promover a divulgação desta PSI, de outros normativos e de ações para disseminar a cultura em segurança da informação, no âmbito do STF;~~

~~IV – atuar de forma harmônica com Núcleo de Prevenção, Tratamento e Resposta a Incidentes em Segurança da Informação do Supremo Tribunal Federal (NPTRI), conforme as diretrizes e objetivos desta Política;~~

~~V – propor novas tecnologias na área de segurança da informação em conformidade com a PSI;~~

~~VI - definir e acompanhar indicadores de aderência à PSI;~~

~~VII – analisar criticamente o andamento dos processos de segurança da informação e apresentar suas considerações ao Comitê de Segurança da Informação.~~

~~Parágrafo único. O Assessor-Chefe da ASI é reconhecido como Gestor de Segurança da Informação do STF~~

~~Art. 12. O Núcleo de Prevenção, Tratamento e Resposta a Incidentes em Segurança da Informação (NPTRI), tem o objetivo de reduzir a probabilidade de ocorrência de incidentes em segurança da informação, prevenindo a ocorrência de incidentes ou minimizando os impactos negativos através do tratamento realizado.~~ (**Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~§ 1º O NPTRI tem como missão gerenciar e manter o processo de gestão de incidentes, de forma a assegurar que as fragilidades e incidentes em segurança da informação sejam identificados e tratados em tempo hábil e de forma padronizada.~~

~~§ 2º O processo de gestão de incidentes será definido em normativo próprio.~~

~~§ 3º O NPTRI é implementado seguindo um modelo misto, sendo composto por membros e especialistas da área.~~

~~I - os membros estão diretamente vinculados ao NPTRI e possuem dedicação exclusiva às atividades de tratamento e resposta a incidentes;~~

~~II – os especialistas da área são servidores da STI que, além das funções relacionadas à área em que estão lotados, desempenham algumas atividades de tratamento e resposta a incidentes;~~

~~III – os membros e especialistas da área são chefiados pelo Supervisor do NPTRI, que será designado entre os membros do NPTRI, juntamente com seu substituto;~~

~~IV – o Supervisor do NPTRI deverá articular com os Gestores de Unidades as atividades que serão desempenhadas pelos especialistas da área;~~

~~V - as habilidades e competências detalhadas dos membros do NPTRI estarão contidas no Manual de Organização da STI, bem como o detalhamento de seus serviços prestados.~~

~~Art. 13. Compete ao NPTRI/STF atuar, principalmente, na coordenação dos aspectos tecnológicos dessa política, tendo a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança da informação, além de armazenar registros para formação de séries históricas, como subsídio estatístico, e para fins de auditoria.~~ (**Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~§ 1º O NPTRI deve observar as orientações e demandas encaminhadas pela ASI com o objetivo de realizar a coordenação dos aspectos tecnológicos da presente política;~~

~~§ 2º O NPTRI deve atuar em ações preventivas, buscando o constante aprimoramento do Tribunal em sua capacidade de resiliência contra ameaças cibernéticas, nos termos desta Política.~~

~~§ 3º Poderá o NPTRI comunicar a ocorrência de incidentes em redes de computadores aos Centros de Tratamento de Incidentes ligados a entidades de governo, ao Centro de Tratamento de Incidentes em Redes de Computadores do Poder Judiciário, tão logo esteja implantado, e ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil - CERT.br, sempre que a cooperação for necessária para prover uma melhor resposta ao incidente.~~

~~§ 4º As atividades do NPTRI equivalem às atividades desempenhadas pela Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR), conforme as normas que regulam o tema na Administração Pública.~~

Art. 14. Compete à unidade responsável pela área de tecnologia da informação: (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~Art. 14. Compete à Secretaria de Tecnologia da Informação (STI~~

I - apoiar a implementação desta PSI;

II - prover os ativos de processamento necessários ao cumprimento desta PSI;

III - propor ações visando à fiscalização da aplicação das normas de segurança da informação vinculadas a esta PSI. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~III - disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho da NPTRI, para implementação da PSI;~~

IV - estabelecer, em conjunto com o CSI/STF, os indicadores de conformidade com a PSI e assegurar que estejam sendo devidamente atualizados; (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~IV - apoiar e buscar os meios para implementar as ações propostas pela Assessoria de Segurança da Informação na execução desta Política;~~

V - analisar criticamente o andamento dos processos de segurança da informação e apresentar suas considerações ao CSI/STF. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~V - executar as orientações e os procedimentos estabelecidos pelo CSI/STF.~~

Art. 14-A. Compete à unidade responsável pela área de segurança cibernética (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**):

I - liderar a proteção dos ativos de TI do STF contra ameaças cibernéticas;

II - monitorar e proteger computadores, sistemas, redes e aplicações no ambiente digital para detecção de ameaças à informação digital e identificação de vulnerabilidades;

III - propor novas tecnologias na área de segurança da informação em conformidade com esta PSI e as normas de segurança vinculadas;

IV - coordenar o processo de gestão de incidentes de segurança da informação, de forma a assegurar que as fragilidades e incidentes de segurança sejam identificados e tratados em tempo hábil e de forma padronizada;

V - propor a elaboração e a revisão de normas e procedimentos inerentes à segurança da informação, bem como analisar periodicamente sua efetividade, nos termos do art. 6º desta PSI;

VI - promover a divulgação desta PSI, de outros normativos e de ações para disseminar a cultura em segurança da informação, no âmbito do STF.

Art. 15. Compete à unidade responsável pela segurança institucional apoiar a implementação da PSI nos aspectos relacionados à segurança física do Tribunal e de seus Ministros, servidores e colaboradores. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~Art. 15. Compete à Secretaria de Segurança apoiar a implementação desta PSI nos aspectos relacionadas com a segurança física do Tribunal e de seus Ministros e servidores~~

Art. 16. Os destinatários dessa PSI, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta Resolução, e têm como deveres:

I - ter pleno conhecimento desta PSI e zelar por seu cumprimento;

II - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;

III - preservar o sigilo da identificação de usuário e senhas de acessos individuais a sistemas de informação, ou outros tipos de credenciais de acesso que lhes forem atribuídos;

IV - participar das campanhas de conscientização e dos treinamentos pertinentes aos temas de segurança da informação e proteção de dados pessoais;

V - reportar qualquer falha ou incidente de segurança da informação de que tiver conhecimento, utilizando o processo estabelecido pelo Tribunal;

VI - utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta PSI e em eventuais normativos subordinados.

Art. 17. As demais Unidades Organizacionais do Tribunal deverão apoiar, observadas suas atribuições regimentais, as estruturas organizacionais responsáveis pela Gestão da Segurança da Informação.

Art. 18. As reuniões ordinárias do CSI/STF serão trimestrais, realizadas com pauta, data e horário definidos previamente e comunicados, com antecedência mínima de 10 (dez) dias.

§ 1º As reuniões deverão ser agendadas preferencialmente ao início de cada trimestre.

§ 2º As deliberações ocorrerão por maioria simples dos participantes, prevalecendo o voto do coordenador em caso de empate, e serão registradas em ata.

§ 3º A forma de comunicação e convocação das reuniões será preferencialmente via meio eletrônico.

Art. 19. Poderão ser realizadas reuniões extraordinárias mediante convocação de qualquer dos membros do CSI/STF.

Art. 20. O CSI/STF poderá convidar outros profissionais para participarem de reuniões ou mesmo do desenvolvimento de trabalhos relacionadas às atribuições do Comitê.

CAPÍTULO IV
DAS COMPETÊNCIAS DA ALTA ADMINISTRAÇÃO

Art. 21. Compete à Presidência do STF:

I - apoiar a aplicação das ações estabelecidas nesta PSI;

II - realizar a nomeação dos membros do CSI/STF. (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~II - realizar as seguintes nomeações:~~

~~a) de membros adicionais do CSI/STF;~~

~~b) do Gestor de Segurança da Informação e seu substituto.~~

~~Art. 22. Compete ao Diretor-Geral nomear os integrantes do NPTRI, composto por membros e especialistas da área indicados pelo Secretário de Tecnologia da Informação.~~ (**Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025)**

~~§ 1º Os membros estão diretamente vinculados ao NPTRI e possuem dedicação exclusiva às atividades de tratamento e resposta a incidentes.~~

~~§ 2º Os especialistas da área são servidores de unidade da STI que, além de suas funções regulares, desempenham algumas atividades de tratamento e resposta a incidentes.~~

~~§ 3º O Supervisor do NPTRI deverá articular com os Gestores de Unidades as atividades que serão desempenhadas pelos especialistas da área.~~

~~Art. 23. Compete ao Diretor-Geral e ao Secretário-Geral:~~ **(Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025)**~~I – aprovar estratégias, normas, procedimentos, planos ou processos que lhe forem submetidos pelo CSI/STF;~~

~~II - submeter à Presidência as propostas que extrapolem sua alçada decisória;~~

~~III - apoiar a aplicação das ações estabelecidas nesta PSI;~~

~~IV - viabilizar financeiramente as ações de implantação desta PSI, inclusive a exequibilidade do Plano de Continuidade de Serviços Essenciais de TI, abrangendo manutenção, treinamento e testes periódicos;~~

~~V - acompanhar os riscos de segurança da informação, com os subsídios fornecidos pelo CSI/STI e disponibilizar recursos para mantê-los em níveis que entendam aceitáveis;~~

~~VI - acompanhar a maturidade em segurança da informação, de acordo com o suporte técnico do CSI/STF, e disponibilizar recursos para aumentá-la quando necessário.~~

CAPÍTULO V

DO PROCESSO DE TRATAMENTO DA INFORMAÇÃO

Art. 24. O tratamento da informação no STF deve englobar as políticas, normas, processos, práticas e instrumentos adotados em todas as etapas do ciclo de vida da informação, o que inclui ações relacionadas à sua produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação e controle.” (NR) (**Redação dada pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)

~~Art. 24. O tratamento da informação deve abranger as políticas, os processos, as práticas e os instrumentos utilizados pelo STF para lidar com a informação ao longo de cada fase do seu ciclo de vida, contemplando o conjunto de ações referentes às fases de produção, recepção, classificação, utilização, acesso, reprodução, transporte,~~

~~transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.~~

Art. 25. As informações produzidas ou custodiadas pelo STF devem ser tratadas em função do seu grau de confidencialidade, criticidade e temporalidade, garantindo-se a sua integridade, autenticidade, disponibilidade e a cadeia de custódia dos documentos.

§ 1º Serão protegidas quanto à confidencialidade as informações classificadas e as que possuem sigilo em decorrência de previsão legal, nos termos da Lei de Acesso à Informação.

§ 2º Serão protegidas quanto à integridade, autenticidade e disponibilidade todas as informações, adotando-se medidas de proteção de acordo com a criticidade atribuída a cada informação.

§ 3º Os direitos de acesso aos sistemas de informação e às bases de dados do Tribunal deverão ser concedidos aos usuários em estrita observância à efetiva necessidade de tal acesso para a execução de suas atividades e funções, observadas, no que couber, as disposições da Lei de Acesso à Informação.

~~Art. 26. Toda informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico.~~ (**Revogado pela Resolução nº 881, de 26 de agosto de 2025, publicada no DJe do dia 1º de setembro de 2025**)~~Parágrafo único. A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pela unidade gestora de riscos, ou pelo Comitê de Segurança da Informação, ou quando prevista em normativo específico.~~

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 27. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal deverão observar, no que couber, as disposições da PSI/STF.

Art. 28. O descumprimento de quaisquer dispositivos da PSI/STF sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 29. Os casos omissos desta PSI serão resolvidos pelo CSI/STF.

Art. 30. A PSI e a Política de Privacidade e Proteção de Dados Pessoais do STF são complementares, devendo ser interpretadas em conjunto.

Art. 31. A PSI/STF será revista no máximo a cada cinco anos, ou por solicitação do CSI, de modo a atualizá-la frente a novos requisitos corporativos.

Art. 32. Fica revogada a Resolução nº 612, de 23 de abril de 2018.

Art. 33. Esta Resolução entra em vigor na data de sua publicação.

Ministro **LUIZ FUX**