SUPERIOR TRIBUNAL DE JUSTIÇA

RESOLUÇÃO STJ/GP N. 12 DE 27 DE ABRIL DE 2023. (*)

Estabelece diretrizes para a Política de Segurança da Informação do Superior Tribunal de Justiça – PSI e revoga a Resolução STJ/GP n. 11 de 12 de novembro de 2015.

A PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA, usando da atribuição conferida pelo art. 21, inciso XXXI do Regimento Interno, considerando o que consta do Processo STJ n. 20.064/2021, e o decidido pelo Conselho de Administração em sessão realizada no dia 8 de novembro de 2023,

CONSIDERANDO a necessidade de revogação da Resolução STJ/GP n. 11 de 12 de novembro de 2015;

CONSIDERANDO que o STJ produz, recebe e custodia informações no exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO a Lei de Acesso à Informação (lei n. 12.527, de 18 de novembro de 2011), que regula o acesso à informação previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

CONSIDERANDO a Resolução CNJ n. 363, de 18 de janeiro de 2021, que estabelece medidas para o processo de adequação à Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a serem adotadas pelos tribunais;

CONSIDERANDO a Resolução CNJ n. 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a necessidade de implementar ações para adequação à Lei Geral de Proteção de Dados Pessoais no que tange à segurança da informação;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à segurança da informação estabelecidas pela NBR ISO/IEC 27000, entre outros padrões sobre o tema reconhecidos no mercado;

CONSIDERANDO a segurança da informação como elemento habilitador dos valores e estratégias institucionais do STJ,

RESOLVE:

Seção I

Das Disposições Iniciais

Art. 1º A Política de Segurança da Informação – PSI do Superior Tribunal de Justiça fica regulamentada por esta resolução.

Parágrafo único. A política de que trata o caput deste artigo se aplica a todos os usuários dos serviços do STJ.

Art. 2º A Política de Segurança da Informação do STJ tem como objetivo garantir a disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e auditabilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelo STJ no exercício de suas atividades.

Seção II

Das Definições

Art. 3º Para os efeitos desta resolução, consideram-se:

I – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II – ativo de informação: parte do patrimônio institucional representado por dado, informação ou conhecimento que sustente um ou mais processos de negócio e tenha valor para a organização;

III – ativos de Tecnologia da Informação e Comunicação – TIC: bens e serviços de tecnologia da informação e comunicação que integrem a infraestrutura tecnológica do Tribunal;

IV – segurança da informação: ações que objetivem assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

V – incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação de dados, sistemas de informação, softwares, dispositivos móveis e dispositivo da infraestrutura de tecnologia da informação de propriedade do STJ, hospedado no datacenter ou na nuvem do STJ, ou sob a guarda do STJ;

VI – incidente crítico de segurança da informação: qualquer incidente de segurança da informação em que for caracterizado grave dano material ou de imagem ao STJ o qual impacte severamente as atividades finalísticas ou os serviços críticos mantidos pelo Tribunal;

VII – usuário de TIC: qualquer pessoa física ou jurídica que utilize os serviços da Secretaria de Tecnologia da Informação e Comunicação, sendo classificado em:

a) interno – ministro, magistrado, servidor (ativo, aposentado, cedido ou licenciado), colaborador ou estagiário que possua identificação na rede de dados do STJ;

b) externo – cidadão, advogado ou fornecedor ou prestador de serviço;

c) instituição – ente público ou privado, compreendendo os órgãos da administração pública direta (indireta, sociedades, empresas privadas ou mistas);

d) instituição integrada – usuários de TIC pertencentes a instituições que possuam soluções de TIC integradas com o STJ;

VIII – informação sigilosa: informação submetida à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, bem como aquelas resguardadas pela legislação;

IX – software: termo genérico usado para descrever programas, aplicativos, scripts, macros e instruções de código embarcado diretamente (BIOS e firmware), de modo a controlar o funcionamento de uma estrutura computacional;

X – gestão de segurança da informação: ações e métodos que visem à integração das atividades de:

a) gestão de riscos;

b) gestão de continuidade de negócios;

c) tratamento de incidentes;

d) tratamento da informação;

e) conformidade;

f) credenciamento;

g) segurança cibernética;

h) segurança física;

i) segurança lógica;

j) segurança orgânica;

k) segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação;

XI – cadeia de custódia: método que preserve a história cronológica, o controle, a transferência e garanta a idoneidade, a fidedignidade, o não repúdio e o rastreamento dos documentos e informações desde a sua criação até a destinação final.

Seção III

Da Estrutura Normativa

Art. 4º São partes integrantes da Política de Segurança da Informação do STJ os normativos e os procedimentos complementares que tenham por objetivo garantir um ambiente controlado e seguro, de modo a oferecer todas as informações necessárias às atividades deste Tribunal.

Parágrafo único. A segurança da informação no STJ abrange aspectos físicos, tecnológicos e humanos.

Art. 5º A estrutura normativa referente à segurança da informação do STJ será estabelecida e organizada da seguinte forma:

I – nível estratégico: política de segurança da informação do STJ, constituída por esta resolução, a qual define as diretrizes fundamentais e os princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico do STJ;

II – nível tático: normativos complementares sobre segurança da informação que contemplem, em seus processos de trabalho, a definição formal dos responsáveis e as obrigações a serem seguidas, bem como, no mínimo, as seguintes diretrizes:

a) gestão de ativos e configuração;
b) gerenciamento de identidade e acesso (físico e lógico);
c) proteção institucional;
d) geração e restauração de cópias de segurança;
e) continuidade de negócio;
f) gestão de incidentes de segurança da informação;
g) gestão de vulnerabilidades;
h) gestão de uso de ativos de TIC;
i) gestão da privacidade e proteção de dados pessoais;
j) desenvolvimento seguro de software;
k) conscientização sobre segurança da informação;

III – nível operacional: procedimentos de segurança da informação que contemplem regras operacionais, roteiros técnicos, fluxos de processos, metodologias, protocolos, manuais com informações técnicas que instrumentalizem o disposto nos normativos referenciados no nível tático, de acordo com as diretrizes e normas de segurança estabelecidas, a fim de permitir sua utilização nas atividades do STJ.

Seção IV

Dos Princípios

Art. 6º São princípios da Política de Segurança da Informação:

I – disponibilidade: propriedade que assegura que a informação está acessível e utilizável, sob demanda, por pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

II – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

III – confidencialidade: propriedade pela qual se assegura que a informação não está disponível ou revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

IV – autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

V – irretratabilidade: propriedade pela qual se assegura que a autoria de uma transação realizada não pode ser negada;

VI – auditabilidade: propriedade pela qual se assegura que a informação é auditável, ou seja, que é possível de ser auditada;

VII – celeridade: oferecimento de respostas rápidas a incidentes e falhas de segurança;

VIII – clareza: atributo pelo qual se assegura que regras, documentação e comunicações de segurança sejam precisas, concisas e de fácil entendimento;

IX – privacidade: respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei n.13.709/2018 (LGPD);

X – responsabilidade: definição clara das responsabilidades primárias e finais pela segurança dos ativos do STJ e pelo cumprimento de processos de segurança;

XI – privilégio mínimo: concessão de autorizações mínimas necessárias para desempenho de uma atividade ou contexto de uso específico;

XII – segregação de funções: separação de atribuições ou responsabilidades entre diferentes perfis de acesso para reduzir as oportunidades de modificação não autorizada ou não intencional, ou de uso indevido dos ativos da organização;

XIII – automação: incentivo à busca de soluções automatizadas de segurança cibernética para obtenção de medições confiáveis, escaláveis e contínuas;

XIV – resiliência: poder de recuperação ou capacidade do STJ de resistir aos efeitos de um incidente, bem como de impedir a reincidência secundária do incidente identificado;

XV – ética: preservação dos direitos e interesses legítimos dos usuários e agentes públicos, sem comprometimento da segurança da informação.

Seção V

Das Diretrizes Gerais

Art. 7º Os ativos de TIC pertencentes ao STJ que estejam disponíveis para os usuários de TIC devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

Art. 8º É vedada a instalação, ativação e uso de ativos de TIC que não tenham sido homologados e/ou adquiridos formalmente pela Secretaria de Tecnologia da Informação e Comunicação do STJ.

Art. 9º. A utilização dos ativos de TIC é passível de monitoramento, auditoria e controle do STJ.

Parágrafo único. Os acessos de administração aos ambientes computacionais do STJ e aos ativos de TIC estarão sujeitos a monitoramentos e controles de segurança adicionais e específicos.

Art. 10. É vedado utilizar os ativos de TIC disponibilizados pelo STJ para acesso, guarda e divulgação de material incompatível com o ambiente do serviço que violem direitos autorais, ou que infrinjam a legislação vigente.

Art. 11. O acesso remoto aos recursos computacionais deve ser realizado mediante adoção dos mecanismos de segurança definidos pela Secretaria de Tecnologia da Informação e Comunicação.

Parágrafo único. O acesso remoto a que se refere o caput deste artigo só poderá ocorrer com a autorização da Secretaria de Tecnologia da Informação e Comunicação, por meio de solicitação formal do titular da unidade requisitante em seus canais de atendimento.

Art. 12. As informações produzidas por usuários de TIC internos no exercício de suas atividades e funções são consideradas patrimônio intelectual do STJ, não cabendo a seus criadores nenhuma forma de direito autoral.

Parágrafo único. Quando as informações forem produzidas por terceiros para uso exclusivo do STJ, os criadores serão obrigados a manter sigilo permanente do conteúdo produzido, por meio de instrumento próprio.

Art. 13. As informações produzidas ou custodiadas pelo STJ devem ser tratadas em função do seu grau de sigilo, criticidade, confiabilidade e temporalidade, garantindo-se a sua integridade, autenticidade, disponibilidade e a manutenção da cadeia de custódia.

Art. 14. Toda informação tratada no STJ será classificada nos termos da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), da Lei Geral de Proteção de Dados e das demais regulamentações vigentes sobre o assunto.

Art. 15. Todo usuário que tratar ativos de informação deverá ser capaz de identificar a classificação dos ativos e, a partir dela, obedecer às restrições de acesso e divulgação associadas.

Art. 16. Os acordos, contratos e outros instrumentos congêneres firmados pelo STJ que envolvam utilização de ativos de informação devem observar o disposto nesta resolução.

Art. 17. As informações sob gestão do STJ devem dispor dos recursos necessários de segurança, de maneira a serem adequadamente protegidas quanto ao acesso e uso.

Parágrafo único. Para as informações consideradas de alta criticidade, serão adotadas medidas especiais de tratamento, com o objetivo de limitar a exploração de informações exclusivas da instituição.

Art. 18. O direito de acesso aos sistemas de informação e às bases de dados do STJ deverá ser concedido aos usuários em estrita observância à necessidade para a execução de suas atividades e funções no STJ.

Art. 19. O acesso aos recursos de TIC será concedido apenas com a solicitação formal do titular da unidade, ou chefe superior, à Secretaria de Tecnologia da Informação e Comunicação.

Art. 20. As credenciais de acesso fornecidas pelo STJ são de uso pessoal e intransferível, vedada a divulgação a terceiros.

Art. 21. A gestão de riscos de segurança da informação deve ser realizada de forma sistemática e contínua e englobar todos os ativos de informação do STJ, com vistas a tratar riscos relacionados à disponibilidade, integridade, confidencialidade e autenticidade.

Art. 22. A segurança física e patrimonial em relação à segurança da informação tem por objetivo prevenir danos e interferências nas instalações do STJ que possam causar perda, roubo ou comprometimento das informações.

Art. 23. A segurança da informação deve auxiliar a manutenção dos processos de gestão de continuidade de negócios do STJ, sobretudo por meio da redução de eventos negativos.

Art. 24. A gestão de incidentes de segurança de informação ocorrerá por meio de processo formal a ser definido em normativo próprio.

Art. 25. Deverão ser instituídas normas que estabeleçam os critérios para a realização de auditorias de conformidade quanto ao cumprimento das ações previstas neste normativo.

Seção VI

Da Estrutura para Governança e Gestão da Segurança da Informação

Art. 26. Integram a estrutura para Governança e Gestão da Segurança da Informação no STJ:

I – Comitê de Governança de Segurança da Informação – CGSI STJ;

II – Gestor de segurança da informação;

III – Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética – ETIR STJ;

IV – Comitê Gestor de Crises Cibernéticas do STJ – CCC STJ.

Art. 27. O Comitê de Governança de Segurança da Informação do STJ será coordenado pelo gestor de segurança da informação e composto pelas/os titulares das seguintes unidades com a respectiva suplência: (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

I - Secretaria do Tribunal; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

II - Secretaria de Tecnologia da Informação e Comunicação; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

III -Assessoria de Conformidade, Integridade e Riscos; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

IV - Coordenadoria de Governança de Dados e Informações Estatísticas; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

V - Secretaria de Polícia Judicial; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

VI – (Revogado pela Resolução STJ/GP n. 28, de 26 de novembro de 2024).

§ 1º (Revogado pela Resolução STJ/GP n. 28, de 26 de novembro de 2024);

§ 2º Os integrantes do Comitê de Governança de Segurança da Informação deverão assinar termo de confidencialidade, em que se comprometerão a

não divulgar as informações restritas ou sigilosas de que venham a ter ciência em razão de sua participação no citado comitê.

§ 3º O Comitê de Governança de Segurança da Informação se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu coordenador.

Art. 28. Compete ao Comitê de Governança de Segurança da Informação:

I – assessorar a administração do STJ em todas as questões relacionadas à segurança da informação;

II – definir, monitorar e propor alterações à Política de Segurança da Informação tornando decisões a respeito de assuntos a ela relacionados, incluindo atividades de priorização de ações e gestão de riscos de segurança; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

III – propor à administração do STJ estratégias para destinação de recursos orçamentários específicos para as ações de segurança da informação;

IV – propor normas internas relativas à segurança da informação;

V – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

VI – consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

VII – propor ações visando à fiscalização da aplicação desta resolução e das normas relacionadas à segurança da informação;

VIII – analisar criticamente o andamento de ações de segurança da informação e a execução dos processos de trabalho, apresentando suas considerações à administração do STJ;

IX – propor à administração do STJ as consequências e as penalidades para os casos de violação desta resolução ou de quebra de segurança, de acordo com as normas acerca do assunto.

Art. 29. Cabe ao gestor de segurança da informação do STJ:

I – coordenar o Comitê de Governança de Segurança da Informação;

II – prestar apoio técnico ao Comitê de Governança de Segurança da Informação, mantendo-o informado de incidentes e níveis de segurança vigentes;

III – coordenar a elaboração e as revisões da política de segurança da informação;

IV – assessorar a administração na implementação da Política de Segurança da Informação;

V – promover ações de capacitação e de profissionalização de recursos humanos relacionados à segurança da informação;

VI – fomentar a divulgação da Política de Segurança da Informação e das normas internas de segurança da informação;

VII – incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VIII – propor recursos necessários às ações de segurança da informação;

IX – acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;

X – acompanhar os trabalhos de auditoria sobre a gestão da segurança da informação e observar os resultados;

XI – acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XII – manter contato direto com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) e com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSIGSI/PR) em assuntos relativos à segurança da informação.

Parágrafo único. O gestor de segurança da informação poderá demandar a execução de ações a servidores ou a unidades da STI quanto à prevenção, tratamento e resposta a incidentes de segurança da informação urgentes, que serão formalmente comunicadas ao gestor da unidade posteriormente.

Art. 30. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética será composta, preferencialmente, por servidores de cargo efetivo, com capacitação técnica compatível com as atividades.

Parágrafo único. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética será criada pelo Diretor-Geral, mediante normativo específico.

Art. 31. Compete à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética coordenar as ações de tratamento e resposta a incidentes de segurança da informação em ambientes de tecnologia da informação e comunicação.

§ 1º Competências adicionais poderão ser atribuídas à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética pelo Diretor-Geral em normativo específico.

§ 2º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética comporá a rede de equipes vinculadas ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

§ 3º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética atuará com competências de comissão.

Art. 32. O Comitê Gestor de Crises Cibernéticas - CCC STJ será coordenado pelo gestor de segurança da informação e composto pelas/os titulares das seguintes unidades com a respectiva suplência: (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

I - Secretaria do Tribunal (presidência); (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

II – (Revogado pela Resolução STJ/GP n. 28, de 26 de novembro de 2024).

III - Secretaria de Tecnologia da Informação e Comunicação; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

IV - Assessoria de Conformidade, Integridade e Riscos; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

V - Assessoria Jurídica do Gabinete do Diretor-Geral; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

VI - Secretaria de Comunicação Social; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

VII - Secretaria de Administração; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

VIII - Secretaria de Polícia Judicial; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

IX – Ouvidoria; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

X – (Revogado pela Resolução STJ/GP n. 28, de 26 de novembro de 2024);

XI – (Revogado pela Resolução STJ/GP n. 28, de 26 de novembro de 2024).

§ 1 º Compõem o Comitê Gestor de Crises Cibernéticas o representante indicado pelo Comitê Gestor da Proteção de Dados Pessoais - CGPD e todos os membros da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética. (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

§ 2° O coordenador poderá convocar servidores que não integrem o comitê para tratar de assunto a ser deliberado; (Redação dada pela Resolução STJ/GP n. 28, de 26 de novembro de 2024)

§ 3º Os integrantes do Comitê Gestor de Crises Cibernéticas deverão assinar termo de confidencialidade, em que se comprometerão a não divulgar as informações restritas ou sigilosas de que tenham conhecimento em razão da participação no comitê.

Art. 33. Compete ao Comitê Gestor de Crises Cibernéticas direcionar e conduzir as ações de tratamento e resposta a incidentes críticos de segurança da informação.

§ 1º A coordenação do Comitê Gestor de Crises Cibernéticas ficará a cargo do Diretor-Geral, que terá autonomia para, em caso de urgência, tomar decisões sobre conteúdos a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações.

§ 2º O Comitê Gestor de Crises Cibernéticas deverá reunir-se tempestivamente sempre que ocorrer um incidente crítico de segurança de informação no âmbito do STJ.

Seção VII

Das Responsabilidades

Art. 34. As unidades do STJ devem atender à política de segurança da informação, observadas as suas atribuições.

Art. 35. É de responsabilidade dos gestores das unidades:

I – indicar a necessidade de treinamento de seus subordinados quanto às normas de segurança da informação;

II – indicar a necessidade de concessão/revogação de credenciais de acesso aos ativos de informação de sua responsabilidade, de acordo com sua classificação;

III – promover a classificação e a restrição de acesso dos ativos de informação sob sua responsabilidade;

IV – determinar o nível de acesso dos seus subordinados e terceiros diante dos ativos de informação sob sua responsabilidade.

Art. 36. Os destinatários desta norma são corresponsáveis pela segurança da informação no STJ e têm como deveres:

I – ter pleno conhecimento da Política de Segurança da Informação e zelar por seu cumprimento;

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

III – participar das campanhas de conscientização e dos treinamentos relativos à segurança da informação e à proteção de dados oferecidos pelo STJ;

IV – reportar qualquer falha ou incidente de segurança da informação de que tiver conhecimento;

V – utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta resolução e em demais normas sobre o assunto;

VI – zelar pelo correto uso dos mecanismos de identificação, autenticação e autorização fornecidos pelo STJ e regras associadas, bem como utilizar de mecanismos de duplo fator de autenticação disponibilizados nos sistemas do Tribunal.

Art. 37. Cabe ao Presidente do STJ:

I – dar suporte à mobilização institucional quanto à conscientização, ao engajamento e à relevância dos temas relativos à política de segurança da informação;

II – apoiar a execução das ações previstas nesta resolução;

III – aprovar propostas de sua competência.

Art. 38. Cabe ao Diretor-Geral:

I – aprovar normas, procedimentos, programas de conscientização, planos e demais questões submetidas pelo Comitê de Governança de Segurança da Informação;

II – submeter ao Presidente do STJ as propostas que extrapolem a sua competência;

III – dar suporte às ações estabelecidas nesta resolução;

IV – viabilizar financeiramente as ações para implantação da Política de Segurança da Informação;

V – nomear o gestor de segurança da informação.

Art. 39. A Secretaria de Gestão de Pessoas deve comunicar imediatamente à Secretaria de Tecnologia da Informação e Comunicação as movimentações, os afastamentos e os desligamentos de servidores e estagiários do STJ, com vista à alteração e/ou exclusão nas permissões de acesso aos recursos de tecnologia.

Art. 40. Os gestores ou os fiscais de contrato que façam uso de serviços digitais ou tenham acesso à rede do STJ deverão comunicar imediatamente à Secretaria de Tecnologia da Informação e Comunicação as ativações, as paralisações e os encerramentos contratuais que impliquem inclusão, alteração e exclusão nas permissões de acesso aos recursos de tecnologia.

Art. 41. É de responsabilidade da Secretaria de Tecnologia da Informação e Comunicação:

I – o uso seguro, a manutenção e a padronização do ambiente computacional do STJ;

II – o controle do uso de todos os tipos de recursos de tecnologia da informação usados pelo STJ, tendo em vista o atendimento dos requisitos técnicos e normativos estabelecidos nesta política.

Seção VIII

Das Disposições Finais

Art. 42. A Política de Segurança da Informação e demais normas, procedimentos, protocolos, planos ou processos associados deverão ser amplamente divulgados em repositórios específicos de acordo com o público-alvo.

Parágrafo único. As diretrizes normativas de que trata o caput deste artigo devem também ser divulgadas aos usuários de TIC internos, quando do seu ingresso ou início da execução do contrato no STJ, bem como aos demais usuários que sejam autorizados a utilizar os recursos de tecnologia da informação e comunicação do STJ.

Art. 43. O descumprimento desta resolução será objeto de apuração da unidade competente nos termos da legislação aplicável, assegurados o contraditório e a ampla defesa.

Art. 44. Os casos omissos serão resolvidos pelo Diretor-Geral da Secretaria do Tribunal.

Art. 45. Esta resolução deverá ser revisada periodicamente, em intervalos de, no máximo, três anos.

Art. 46. Fica revogada a Resolução STJ/GP n. 11 de 12 de novembro de 2015.

Art. 47. Esta resolução entra em vigor na data de sua publicação.

Ministra MARIA THEREZA DE ASSIS MOURA

(*) Republicada em decorrência de decisão do Conselho de Administração do STJ, em sessão realizada no dia 8 de novembro de 2023, presidida pela Ministra Maria Thereza de Assis Moura.