RESOLUÇÃO STJ/GP N. 11 DE 12 DE NOVEMBRO DE 2015.

Institui a política de segurança da informação do Superior Tribunal de Justiça e dá outras providências.

O PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA, usando da atribuição conferida pelo art. 21, inciso XX, do Regimento Interno e considerando as boas práticas em segurança da informação preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011 e 27014:2013, bem como o que consta do Processo STJ n. 22.598/2015 e o decidido pelo Conselho de Administração na sessão de 11 de novembro de 2015,

RESOLVE:

Art. 1º A política de segurança da informação do Superior Tribunal de Justiça fica instituída por esta resolução.

§ 1º Os usuários internos e externos de informações produzidas ou custodiadas pelo Tribunal estão sujeitos às disposições estabelecidas na política de segurança da informação.

§ 2º As ações da política de segurança da informação serão implementadas e acompanhadas pelas unidades do Tribunal.

Seção I
Das Disposições Preliminares

Art. 2º Para os efeitos desta resolução, consideram-se:

I – confidencialidade: garantia de que a informação seja acessada somente pelas pessoas que tenham autorização para tal;

II – custodiante: servidor, unidade ou estrutura *ad hoc* que detenha a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal;

III – disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos e sistemas autorizados;

IV – gestor da informação: servidor, unidade ou estrutura *ad hoc* que, no exercício de suas competências, seja responsável pela produção de informações, pela definição de requisitos de soluções de tecnologia da informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues ao Tribunal;

V – incidente em segurança da informação: fraude, sabotagem, desvio, falha de equipamentos, acessos não autorizados, mau uso, extravio, furto ou evento indesejado ou inesperado que possa comprometer as atividades do Tribunal ou ameaçar a

segurança da informação;

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

VII – integridade: qualidade da informação não modificada, inclusive quanto à origem, ao trânsito e ao destino;

VIII – segurança da informação: proteção da informação contra ameaças para garantir a continuidade das atividades do Tribunal e minimizar os riscos;

IX – usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não seja caracterizada como usuário interno;

X – usuário interno: qualquer servidor, prestador de serviço, estagiário ou qualquer outro colaborador que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal.

Art. 3º A segurança da informação no Superior Tribunal de Justiça abrange aspectos físicos, tecnológicos e humanos e orienta-se pelos princípios da confidencialidade, disponibilidade e integridade.

Seção II
Do Uso dos Recursos de Tecnologia da Informação

Art. 4º Os recursos de tecnologia da informação disponibilizados nas unidades do Tribunal destinam-se, exclusivamente, ao atendimento das necessidades do serviço.

§ 1º É proibida a utilização dos recursos de tecnologia da informação disponibilizados pelo Tribunal para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais, ou que infrinja a legislação vigente.

§ 2º É vedada a instalação de recursos de tecnologia da informação que não tenham sido homologados e/ou adquiridos pelo Tribunal.

Art. 5º Compete à Secretaria de Tecnologia da Informação e Comunicação - STI prover e controlar o uso dos recursos de tecnologia da informação, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional.

Art. 6º Aos usuários são fornecidos mecanismos de identificação, autenticação e autorização baseados em conta e senha e/ou certificação digital, de uso pessoal e intransferível, vedada sua divulgação a terceiros.

§ 1º Pelo uso indevido dos mecanismos de identificação respondem quem permitiu ou facilitou o acesso e quem os utilizou.

§ 2º O acesso aos recursos de tecnologia da informação é concedido mediante solicitação de titular de unidade do Tribunal à Secretaria de Tecnologia da Informação e Comunicação.

§ 3º Todas as operações realizadas com uso dos recursos de tecnologia da informação serão registradas para fins de auditoria.

§ 4º A Secretaria de Gestão de Pessoas deve comunicar imediatamente à Secretaria de Tecnologia da Informação e Comunicação as movimentações, afastamentos e desligamento de servidores e estagiários do Tribunal para fins de alteração nas permissões de acesso aos recursos de tecnologia.

§ 5º Os titulares das unidades do Tribunal devem pessoalmente realizar, quando possível, ou solicitar imediatamente à Secretaria de Tecnologia da Informação e Comunicação a alteração nas permissões de acesso aos recursos de tecnologia dos servidores, estagiários e prestadores de serviço sob sua responsabilidade, sempre que houver necessidade e quando ocorrer violação do disposto nesta resolução.

§ 6º A Secretaria de Tecnologia da Informação e Comunicação realizará as alterações nas permissões de acesso no mesmo dia do recebimento da demanda, ou até o expediente seguinte no caso de chamados abertos após as 16h, dando imediata ciência ao demandante quanto à efetivação do procedimento.

Seção III
Do Comitê Gestor e da Comissão Técnica de Segurança da Informação

Art. 7º Ficam criados o Comitê Gestor e a Comissão Técnica de Segurança da Informação.

§ 1º O Comitê Gestor de Segurança da Informação (CGSI), colegiado de natureza consultiva e de caráter permanente, tem por objetivo estabelecer modelo de gestão que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) apoiado pela Política de Segurança, Normas e Procedimentos.

§ 2º A Comissão Técnica de Segurança da Informação (CTSI), de natureza executiva e subordinada ao Comitê Gestor de Segurança da Informação, tem por objetivo implantar, manter e operacionalizar o Sistema de Gestão de Segurança da Informação (SGSI).

Art. 8º O Comitê Gestor de Segurança da Informação (CGSI) será composto pelo Diretor-Geral da Secretaria do Tribunal (Coordenador), pelo Secretário-Geral da Presidência e pelos titulares das seguintes unidades:

I – Assessoria de Modernização e Gestão Estratégica;

II – Assessoria Jurídica;

III – Secretaria de Administração;

IV – Secretaria de Comunicação Social;

V – Secretaria de Controle Interno;

VI – Secretaria de Documentação;

VII – Secretaria de Gestão de Pessoas;

VIII – Secretaria de Gestão Predial;

IX – Secretaria de Jurisprudência;

X – Secretaria de Orçamento e Finanças;

XI – Secretaria de Segurança;

XII – Secretaria de Serviços Integrados de Saúde;

XIII – Secretaria de Tecnologia da Informação e Comunicação;

XIV – Secretaria dos Órgãos Julgadores;

XV – Secretaria Judiciária.

§ 1º As reuniões ordinárias do CGSI serão realizadas semestralmente com quórum mínimo de nove membros, incluído o Coordenador.

§ 2º Poderão ser realizadas reuniões extraordinárias sempre que forem convocadas por seu Coordenador.

§ 3º O trabalho do CGSI se dará sem prejuízos das atribuições ordinárias de seus membros e não implica, em nenhuma hipótese ou a qualquer título, remuneração complementar.

Art. 9º A Comissão Técnica de Segurança da Informação (CTSI) será integrada por servidores indicados pelas seguintes unidades do Tribunal:

I – Secretaria de Tecnologia da Informação e Comunicação – três membros;

II – Secretaria de Segurança – um membro;

III – Secretaria de Documentação – um membro;

IV – Secretaria Judiciária – um membro;

V – Secretaria dos Órgãos Julgadores – um membro.

§ 1º O coordenador da Comissão Técnica será definido entre os integrantes da Secretaria de Tecnologia da Informação e Comunicação.

§ 2º As reuniões da CTSI serão realizadas com quórum mínimo de quatro membros sempre que convocadas por seu Coordenador.

§ 3º O trabalho da CTSI se dará sem prejuízos das atribuições ordinárias de seus membros e não implica, em nenhuma hipótese ou a qualquer título, remuneração complementar.

§ 4º A designação dos integrantes da comissão técnica será realizada pelo Diretor-Geral, mediante indicação dos titulares das unidades mencionadas no caput.

Seção IV
Das Competências e Responsabilidades

Art. 10. Compete ao Comitê Gestor de Segurança da Informação:

I – definir modelo de gestão de segurança da informação e fomentar sua aplicação;

II – propor metas e ações corporativas em segurança da informação;

III – definir critérios e parâmetros de avaliação de conformidade da gestão e execução de serviços de segurança da informação;

IV – definir critérios, gerenciar e avaliar os resultados de auditorias de conformidade de segurança da informação e de aspectos legais relacionados à proteção

das informações do Tribunal;

V – definir ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de segurança da informação;

VI – propor a elaboração e a revisão de políticas, normas e procedimentos inerentes à segurança da informação.

Art. 11. Compete à Comissão Técnica de Segurança da Informação:

I – implantar, manter e operacionalizar o Sistema de Gestão de Segurança da Informação (SGSI);

II – elaborar e submeter à Secretaria do Tribunal estudos sobre planejamento, controle, políticas e ações de segurança da informação;

III – elaborar e submeter à Secretaria do Tribunal proposta de normas e procedimentos complementares a esta Política de Segurança da Informação;

IV – coordenar e acompanhar a implementação de ações sobre segurança da informação;

V – monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal;

VI – apoiar as unidades do Tribunal na adoção de medidas que garantam a continuidade das suas atividades e o retorno à situação de normalidade em caso de incidente em segurança da informação;

VII – coordenar ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de segurança da informação, com apoio das demais unidades do Tribunal.

Art. 12. Compete ao gestor da informação:

I – adotar critérios de classificação e procedimentos de acesso às informações, observados os dispositivos legais e normas internas referentes ao sigilo e a outros requisitos de classificação;

II – propor regras específicas para o uso das informações.

Art. 13. Compete ao custodiante da informação:

I – zelar pela segurança da informação sob sua custódia, conforme os critérios definidos pelo respectivo gestor da informação;

II – comunicar tempestivamente ao gestor da informação situações que comprometam a segurança das informações sob sua custódia;

III – comunicar ao gestor eventuais limitações ao cumprimento dos critérios definidos para segurança da informação.

Art. 14. Compete às unidades do Tribunal:

I – implementar e acompanhar ações da política de segurança da informação;

II – colaborar na conscientização dos usuários internos em relação aos conceitos e às práticas de segurança da informação;

III – incorporar aos processos de trabalho práticas inerentes à segurança da

informação;

IV – adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de violação à política de segurança da informação por parte dos usuários internos.

Art. 15. Os usuários internos devem zelar pela segurança das informações a que tenham acesso e comunicar ao Comitê Gestor de Segurança da Informação os incidentes de que tenham conhecimento.

Seção V
Das Disposições Finais

Art. 16. O acesso e a classificação das informações produzidas ou custodiadas pelo Tribunal são os estabelecidos na regulamentação interna da Lei de Acesso à Informação.

Art. 17. As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual do Tribunal e não cabe a seus criadores qualquer forma de direito autoral.

Parágrafo único. Quando as informações forem produzidas por terceiros para uso exclusivo do Tribunal, a obrigatoriedade do seu sigilo deve ser estabelecida em instrumento adequado.

Art. 18. As normas relacionadas à segurança da informação editadas pelo Tribunal deverão observar as disposições estabelecidas nesta resolução.

Art. 19. A inobservância dos dispositivos desta resolução pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 20. Fica revogada a Portaria n. 25 de 1º de fevereiro de 2008.

Art. 21. Esta resolução entra em vigor na data de sua publicação.

Ministro FRANCISCO FALCÃO