

RESOLUÇÃO Nº 396, DE 23 DE ABRIL DE 2009

Estabelece diretrizes para a segurança da informação do Supremo Tribunal Federal e dá outras providências.

O PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, nos termos do artigo 361, inciso I, do Regimento Interno, tendo em vista o contido no Processo nº 331.217/2008,

considerando que o Tribunal, no exercício de suas competências, gera, adquire e absorve informações, que devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

considerando que as informações no Tribunal são armazenadas em diferentes meios, veiculadas por diferentes formas e, portanto, vulneráveis a incidentes em segurança da informação;

considerando que a adequada gestão da informação precisa nortear todos os processos de trabalho e deve ser impulsionada por política corporativa de segurança da informação;

RESOLVE:

Art. 1º A atividade de segurança da informação no Supremo Tribunal Federal abrange aspectos físicos, tecnológicos e humanos e orienta-se pelos seguintes princípios:

I - confidencialidade: garante que a informação seja acessada somente pelas pessoas que tenham autorização para tal;

II - disponibilidade: garante que as informações estejam acessíveis às pessoas autorizadas, no momento requerido;

III - integridade: garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.

Art. 2º Para os efeitos desta Resolução, ficam estabelecidas as seguintes conceituações:

I - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado

contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

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

III - 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;

IV - custodiante: servidor, unidade ou estrutura *ad hoc* que detenha a posse, mesmo que transitória, de informação produzida ou recebida pelo 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 - usuário interno: qualquer servidor, ocupante de posto de trabalho, prestador de serviço terceirizado, estagiário ou qualquer outro colaborador que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo STF;

VII - 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.

Art. 3º Os usuários internos e externos que, de forma autorizada, tenham acesso a informações produzidas ou custodiadas pelo STF estão sujeitos às disposições sobre segurança da informação constantes desta Resolução e demais normativos.

Art. 4º Compete ao Comitê Gestor de Segurança da Informação do Supremo Tribunal Federal gerir a segurança das informações do STF, bem como:

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

II - apresentar à Secretaria do Tribunal os resultados da segurança da informação;

III - 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 STF;

IV - definir critérios e parâmetros de avaliação de conformidade da gestão e execução de serviços de segurança da informação;

V - coordenar e acompanhar a implementação de ações sobre segurança da informação;

VI - monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal;

VII - 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;

VIII - 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.

Parágrafo único. Cabe às unidades do Tribunal implementar e acompanhar ações de segurança da informação nas respectivas áreas de atuação.

Art. 5º Compete ao gestor da informação:

I - definir 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. 6º 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 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. 7º Compete aos titulares das unidades do Tribunal, no que se refere à segurança da informação:

I - colaborar na conscientização dos usuários internos sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade práticas inerentes à segurança da informação;

III - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários internos sob sua supervisão.

Art. 8º Compete aos usuários internos garantir a segurança das informações a que tenham acesso e comunicar ao Comitê Gestor de Segurança da Informação os incidentes de que tenham conhecimento.

Art. 9º O acesso às informações produzidas ou custodiadas pelo Tribunal, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários.

Parágrafo único. Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários necessitará de prévia autorização formal do gestor da informação.

Art. 10. As medidas de segurança da informação devem ser planejadas, aplicadas, implementadas e, periodicamente, reavaliadas de acordo com os

objetivos institucionais e os riscos para as atividades do STF.

Art. 11. A classificação das informações produzidas ou custodiadas pelo Tribunal deve indicar a necessidade, a prioridade e o grau de proteção dessas informações, durante todo o seu ciclo de vida, com níveis e critérios para sua criação, manuseio, transporte, armazenamento e descarte.

Art. 12. As informações produzidas por usuários internos, no exercício de suas funções, são patrimônio intelectual do STF 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. 13. As normas editadas pelo Tribunal, relacionadas à segurança da informação, deverão observar as disposições estabelecidas nesta Resolução.

Art. 14. A inobservância dos dispositivos desta Resolução pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 15. Fica revogado o art. 2º da Resolução nº 371, de 18 de julho de 2008.

Art. 16. Esta Resolução entra em vigor na data de sua publicação.

Ministro GILMAR MENDES

Este texto não substitui a publicação oficial.