

ANEXO À RESOLUÇÃO 610, DE 23 DE ABRIL DE 2018

Cargos Efetivos do Quadro de Pessoal do Supremo Tribunal Federal

CARGO	ÁREA DE ATIVIDADE	ESPECIALIDADE	QUANTIDADE
Analista Judiciário	Judiciária		326
		Oficial de Justiça Avaliador Federal	5
	Administrativa		81
		Contabilidade	13
		Segurança Judiciária	1
	Apoio Especializado	Análise de Informática	20
		Análise de Sistemas de Informação	29
		Arquitetura	3
		Arquivologia	2
		Biblioteconomia	20
		Comunicação Social	5
		Enfermagem	4
		Engenharia Civil	3
		Engenharia Elétrica	4
		Engenharia Mecânica	1
		Estatística	1
		Fisioterapia	4
		Medicina	14
		Nutrição	1
		Odontologia	8
		Pedagogia	1
		Psicologia	4
	Revisão de Textos	14	
	Serviço Social	3	
	Suporte em Tecnologia da Informação	16	
	Taquigrafia*	11	
	Subtotal		
Técnico Judiciário	Administrativa		394
		Carpintaria e Marcenaria*	4
		Copeiragem*	1
		Mecânica*	3
		Segurança Judiciária	61
		Telecomunicações e Eletricidade*	3
	Telefonia*	2	
	Apoio Especializado	Enfermagem	3
		Tecnologia da Informação	70
	Subtotal		
TOTAL			1.135

* Especialidades em extinção.

RESOLUÇÃO 611, DE 23 DE ABRIL DE 2018

Altera a Resolução 587, de 29 de julho de 2016.

A PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, no uso das atribuições que lhe conferem os arts. 13, inc. XIX, e 363, inc. I, do Regimento Interno do Tribunal, o art. 218, XV, do Regulamento da Secretaria, e a deliberação tomada em Sessão Administrativa de 22 de junho de 2016,

RESOLVE:

Art. 1º Fica acrescido o seguinte dispositivo à Resolução 587, de 29 de julho de 2016:

Art. 2º

§ 6º Prorroga-se automaticamente o prazo do § 1º deste artigo para o primeiro dia útil subsequente quando o término da contagem for em dia sem expediente na Secretaria do Tribunal.

Art. 2º Esta Resolução entrará em vigor na data de sua publicação.

Ministra CÁRMEN LÚCIA

RESOLUÇÃO 612, DE 23 DE ABRIL DE 2018

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

A 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 que a segurança é aspecto essencial para a adequada gestão da informação;

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 e 27014:2013; e

CONSIDERANDO que a Norma Técnica ABNT NBR ISO/IEC 27002:2013 recomenda revisões periódicas da política de segurança da informação das Instituições;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política Corporativa de Segurança da Informação do Supremo Tribunal Federal (PCSI/STF) contempla os princípios, objetivos e diretrizes estabelecidos nesta Resolução, observadas as disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. Autoridades, servidores, colaboradores e usuários externos deverão observar as diretrizes, normas e procedimentos de segurança da informação concernentes à Política de que trata esta Resolução, e serão responsáveis por garantir a segurança das informações a que tenham acesso.

Art. 2º Para os efeitos desta Resolução, entende-se por:

I - ativo de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II - autenticidade: princípio da segurança da informação com vistas a assegurar a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

III - autoridade: Ministros, juízes e dignitários;

IV - ciclo de vida da informação: compreende etapas e eventos de produção, recepção, utilização, acesso, alteração, reprodução, transporte, transmissão, distribuição, destinação, arquivamento e eliminação da informação;

V - classificação da informação: ação consistente em definir o nível de sensibilidade da informação a fim de assegurar que esta receba o nível adequado de proteção, conforme valor, requisitos legais e criticidade para a Instituição;

VI - colaborador: qualquer ocupante de posto de trabalho, prestador de serviço, estagiário ou qualquer outra pessoa que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo STF e às dependências do Tribunal;

VII - servidor: ocupante de cargo efetivo ativo, servidor aposentado, requisitado, cedido ou ocupante de cargo em comissão;

VIII - confidencialidade: princípio da segurança da informação que visa garantir que a informação seja acessada somente por pessoas, processos ou sistemas que possuam autorização para tal;

IX - custodiante da informação: servidor, unidade ou estrutura *ad hoc* que detenha a guarda, mesmo que transitória, de informação produzida ou recebida pelo Tribunal; não faz parte, em geral, do grupo de acesso e, portanto, não está autorizado a acessar a informação;

X - disponibilidade: princípio da segurança da informação a fim de garantir que as informações estejam acessíveis às pessoas, aos processos e aos sistemas autorizados, no momento requerido;

XI - gestor da informação: autoridade, 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;

XII - incidente em segurança da informação: ocorrência ou série de ocorrências que indiquem uma possível violação da política de segurança da informação ou falhas de controles, com potencial e probabilidade de comprometer as operações do negócio e/ou ameaçar a segurança da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIII - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIV - integridade: princípio da segurança da informação de modo a garantir a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;

XV - segurança da informação: proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade ou autenticidade, para minimizar riscos, garantir a eficácia das ações institucionais e preservar a imagem do STF;

XVI - sensibilidade: grau de sigilo necessário para a informação;

XVII - sistema de gestão de segurança da informação: conjunto de elementos organizados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;

XVIII - tratamento da informação: conjunto de ações referentes ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo todas as etapas do seu ciclo de vida; e

XIX - usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo STF, ou a sistemas de conexão à internet disponibilizados pelo Tribunal, e que não seja caracterizada como colaborador, servidor ou autoridade.

Art. 3º A PCSI/STF tem por finalidade assegurar a proteção dos ativos de informação do Tribunal contra ameaças e vulnerabilidades, e por objetivos estabelecer princípios e diretrizes, responsabilidades e competências, bem como definir normas e procedimentos específicos de segurança da informação que nortearão, observadas as estratégias organizacionais e as diretrizes da segurança institucional, a implementação do

Sistema de Gestão de Segurança da Informação do STF (SGSI/STF).

Art. 4º A segurança da informação tem como princípios:

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 sua proteção adequada;

IV - garantia da disponibilidade das informações custodiadas;

V - transparência das informações públicas; e

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

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos e humanos do Tribunal.

CAPÍTULO II DA ESTRUTURA DA POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

Art. 5º A PCSI/STF é composta pelos seguintes temas:

I - classificação da informação;

II - gestão de incidentes em segurança da informação;

III - controle de acesso à informação;

IV - segurança em recursos humanos, conscientização e capacitação em segurança da informação;

V - gestão de áreas seguras;

VI - gestão de equipamentos;

VII - gestão de ativos;

VIII - gestão de cópias de segurança;

IX - gestão de dispositivos móveis e trabalho remoto; e

X - análise crítica da segurança da informação.

Parágrafo único. Os temas listados no *caput*, e outros que venham a surgir, serão definidos em normativos específicos, a ser estruturados e monitorados de forma a permitir sua melhoria contínua.

CAPÍTULO III DAS COMPETÊNCIAS E DAS RESPONSABILIDADES

Art. 6º Cabe à Secretaria do Tribunal e à Secretaria-Geral da Presidência, atuando em conjunto, fomentar e patrocinar as ações relacionadas à implantação e à manutenção da PCSI.

Art. 7º Fica instituído o Comitê Corporativo de Segurança da Informação (CCSI), órgão colegiado, de natureza deliberativa, cuja composição será definida em normativo específico, ao qual compete:

I - indicar as necessidades corporativas de segurança da informação;

II - propor a elaboração e a revisão de políticas, diretrizes, normas e procedimentos inerentes à segurança da informação, bem como analisar periodicamente sua efetividade;

III - manifestar-se sobre propostas de alteração, de revisão da PCSI/STF, minutas de normativos e 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;

IV - propor a implementação de ações corporativas de segurança da informação e o acompanhamento de seus resultados;

V - promover a definição, a implantação, o monitoramento e a revisão do Sistema de Gestão de Segurança da Informação do STF (SGSI/STF); e

VI - promover a divulgação de boas práticas de segurança da informação.

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

§ 2º Deverão integrar o CCSI as unidades custodiantes de informações relevantes do Tribunal, objetivamente identificadas.

Art. 8º Fica instituído o Comitê Executivo de Segurança da Informação (CESI), de natureza executiva, cuja composição será definida em normativo específico e ao qual compete:

I - gerenciar e monitorar o Sistema de Gestão de Segurança da Informação do STF (SGSI/STF), bem como propor as adaptações necessárias para garantir sua melhoria contínua;

II - coordenar e acompanhar a implementação do SGSI/STF e das normas complementares de segurança da informação;

III - apresentar ao CCSI proposta de revisão da PCSI/STF para atualizá-la frente a novos requisitos corporativos;

IV - apoiar as unidades do Tribunal na definição de processos de trabalho e de procedimentos operacionais necessários à proteção de suas informações;

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

VI - coordenar, com o apoio da Secretaria de Gestão de Pessoas (SGP), e demais unidades competentes, ações permanentes de divulgação, treinamento, educação e conscientização das autoridades, servidores e colaboradores, em relação aos conceitos e às práticas de segurança da informação em toda a sua abrangência.

Art. 9º Sobre a gestão de incidentes em segurança da informação, compete à cada unidade do Tribunal, às autoridades, aos servidores e aos colaboradores contribuir, no exercício de suas atribuições e competências, na prevenção, na identificação, no encaminhamento e no tratamento de incidentes em segurança da informação.

Parágrafo único. As competências relacionadas à gestão de incidentes em segurança da informação serão definidas em normativo específico.

Art. 10. Cabe ao gestor da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pelo STF:

I - garantir sua segurança;

II - definir os requisitos de segurança da informação necessários ao negócio, com base em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho;

III - propor regras específicas para o seu uso; e

IV - classificá-las, a partir de critérios pertinentes, e definir procedimentos para o acesso, observados os dispositivos legais e regimentais relativos à confidencialidade.

§ 1º Caberá ao Presidente e aos Ministros, a qualquer tempo, indicar, orientar e autorizar procedimentos que visem a garantir a segurança da informação nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação.

§ 2º Havendo dúvida quanto ao gestor de informação, sua indicação competirá ao Diretor-Geral da Secretaria.

Art. 11. São responsabilidades do custodiante da informação:

I - garantir a segurança da informação sob sua guarda, conforme os critérios definidos pelo respectivo gestor da informação;

II - comunicar tempestivamente ao gestor da informação acerca das situações que comprometam a segurança das informações; e

III - comunicar ao gestor da informação eventuais limitações para o cumprimento dos critérios por ele definidos com vistas à proteção da informação.

Art. 12. Compete aos gestores das unidades do Tribunal:

I - sensibilizar autoridades, servidores e quaisquer colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

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

III - implementar as medidas administrativas necessárias para que sejam adotadas ações preventivas ou corretivas em tempo hábil em caso de comprometimento da segurança da informação.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 13. 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 parágrafo anterior pelos colaboradores do STF em projetos ou atividades diversas daquelas estabelecidas pelo Tribunal, salvo autorização específica dos Ministros nos processos e documentos de sua competência, ou do Presidente, nos demais casos.

Art. 14. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal deverão observar, no que couber, as disposições da PCSI/STF.

Art. 15. O descumprimento de quaisquer dispositivos da PCSI/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. 16. A PCSI/STF será revista no máximo a cada cinco anos, ou por solicitação do CCSI, de modo a atualizá-la frente a novos requisitos corporativos.

Art. 17. Os normativos específicos a que se referem o art. 5º, parágrafo único, o art. 7º, *caput*, o art. 8º, *caput*, e o art. 9º, parágrafo único, desta Resolução, de caráter integrativo, serão de competência do Diretor-Geral da Secretaria e deverão ser publicadas no prazo máximo de noventa dias.

Art. 18. Revogam-se as Resoluções 396, de 23 de abril de 2009, 507, de 28 de junho de 2013, 575, de 31 de março de 2016 e 588, de 5 de agosto de 2016.

Art. 19. Esta Resolução entra em vigor na data de sua publicação.

Ministra **CÁRMEN LÚCIA**

RESOLUÇÃO 613, DE 23 DE ABRIL DE 2018

Regulamenta a divulgação e a atualização das informações na página *Transparência* no sítio do Supremo Tribunal Federal na internet.

A PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o que consta dos Processos Administrativos eletrônicos 3698/2016 e 9379/2016,

CONSIDERANDO o princípio da publicidade, estabelecido no art. 37 da Constituição da República,

CONSIDERANDO a Lei Complementar 101/2000, a Lei 12.527/2011, a Resolução 528/2014 e a Sessão Administrativa realizada em 22 de maio de 2012,

R E S O L V E:

Art. 1º A divulgação e a atualização das informações na página *Transparência*, do sítio eletrônico do Supremo Tribunal Federal - STF ficam regulamentadas por esta Resolução.

Art. 2º Serão divulgadas na página *Transparência*, independentemente de requerimento, as informações relativas:

- I - ao STF, de interesse geral e coletivo;
- II - à gestão orçamentária e financeira;
- III - às compras, licitações e contratos;
- IV - à gestão de pessoas;
- V - à gestão estratégica.