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 terá a seguinte composição:

I – Diretor-Geral (coordenador);

II – representante indicado pelo Comitê Gestor da Proteção de Dados Pessoais – CGPD;

III – titular da Secretaria de Tecnologia da Informação e Comunicação;

IV – gestor de segurança da informação;

V – todos os membros da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;

VI – titular ou representante da Assessoria de Conformidade e Integridade Digital;

VII – titular ou representante da Assessoria Jurídica do Gabinete do Diretor-Geral;

VIII – titular ou representante da Secretaria de Comunicação Social;

Texto de acordo com a publicação na fonte oficial (DJe do STJ, 7 jul. 2023. Republicado em 9 nov. 2023)
Edição nº 3754 - Brasília, Disponibilização: quarta-feira, 08 de novembro de 2023 Publicação: quinta-feira, 09 de novembro de 2023
Código de Controle do Documento: 3231FDDD-8C7B-4863-B8BD-E40205C633EF

IX – titular ou representante da Secretaria de Administração;

X – titular ou representante da Secretaria de Polícia Judicial;

XI – titular ou representante da Ouvidoria.

§ 1º O coordenador poderá convocar servidores que não integrem o comitê para tratar de assunto a ser deliberado.

§ 2º Os representantes titulares e substitutos, indicados pelas unidades citadas neste artigo, devem ser preferencialmente servidores efetivos e serão designados, mediante portaria, pelo Diretor-Geral.

§ 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.

Texto de acordo com a publicação na fonte oficial (DJe do STJ, 27 jul. 2023. Republicado em 9 nov. 2023)

Edição nº 3754 - Brasília, Disponibilização: quarta-feira, 08 de novembro de 2023 Publicação: quinta-feira, 09 de novembro de 2023
Código de Controle do Documento: 3231FDDD-8C7B-4863-B8BD-E40205C633EF