INSTRUÇÃO NORMATIVA STJ/GDG N. 17 DE 26 DE OUTUBRO DE 2021.

Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) – do Superior Tribunal de Justiça.

O DIRETOR-GERAL DA SECRETARIA DO SUPERIOR TRIBUNAL DE JUSTIÇA, usando da atribuição conferida pelo item 17.2, inciso X, alínea "b", do Manual de Organização do Superior Tribunal de Justiça e considerando o que consta do Processo SEI STJ n. 7.575/2021,

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 Resolução STJ n. 11 de 12 de novembro de 2015, que institui a Política de Segurança da Informação do Superior Tribunal de Justiça,

RESOLVE:

Seção I
Das Disposições Iniciais

Art. 1º A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR no STJ fica instituída por esta Instrução Normativa.

Parágrafo único. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação tem como missão:

I – facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança da informação em ambientes de tecnologia da informação e comunicação;

II – responder às notificações e armazenar registros para a formação de séries históricas, como subsídio estatístico, para fins forenses e de auditoria.

Art. 2º São objetivos da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação:

I – monitorar as redes de computadores;

Edição nº 3262 - Brasília, Disponibilização: Quinta-feira, 28 de Outubro de 2021 Publicação: Quarta-feira, 03 de Novembro de 2021
Código de Controle do Documento: 14141C51-9301-40D8-A5E5-65A128CC458E

II – detectar e analisar ataques;

III – tratar incidentes, vulnerabilidades e artefatos maliciosos;

IV – recuperar sistemas;

V – prover e incentivar a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais.

Art. 3º Para os efeitos desta instrução normativa consideram-se:

I – dispositivo de infraestrutura de tecnologia da informação: qualquer dispositivo eletrônico utilizado para comunicação e processamento de dados tais como:

a) equipamentos servidores;

b) *appliances;*

c) *softwares*;

d) *switches;*

e) roteadores;

f) *storages;*

g) firewalls;

h) *instrusion Prevention System* – IPS;

i) e-mail *gateway*, entre outros, que atue como provedor de serviços de tecnologia da informação e comunicação – TIC para os usuários finais;

II – dispositivos móveis: qualquer dispositivo eletrônico para processamento de dados portátil de propriedade do STJ, destinado ao usuário final para utilização, tais como *tablets, notebooks e smartphones*;

III – *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;

IV – artefato malicioso: qualquer *software* ou parte de um *software* construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e redes de computadores;

V – incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação de dados pessoais, *softwares,* dispositivos móveis e dispositivo de 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, onde reste evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

VII – tratamento e resposta de incidentes de segurança: contempla as ações definidas no plano de resposta a incidentes do STJ com o objetivo de isolar e eliminar o evento malicioso, recuperar o ambiente, documentar o ocorrido e protegê-lo contra novos incidentes de segurança da informação;

VIII – vulnerabilidade: qualquer fragilidade dos *softwares*, dispositivos móveis e dispositivos de infraestrutura de tecnologia da informação que permitam a exploração maliciosa e acessos indesejáveis e não autorizados;

IX – usuário: qualquer indivíduo ou organização que utiliza ou trabalha com algum sistema, dispositivo ou serviço de TIC oferecido pelo STJ;

X – registros: informações sobre a quantidade e o tipo dos alertas e incidentes de segurança da informação.

Seção II
Das Atribuições

Art. 4º Compete à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação:

I – receber, analisar e classificar os logs de segurança para identificar os incidentes de segurança da informação;

II – coordenar as atividades de tratamento e respostas a incidentes de segurança da informação;

III – definir o plano de resposta a incidentes, com os procedimentos a serem executados e as medidas de recuperação a serem adotadas quando da ocorrência de incidentes de segurança da informação;

IV – comunicar ao Comitê de Crises Cibernéticas do STJ a ocorrência de incidente crítico de segurança da informação e apoiar nas ações de tratamento e resposta inerentes a esta situação;

V – acionar e prestar de maneira continua informações técnicas assertivas à alta administração do Tribunal e a quem ela determinar quando da condução, do tratamento e da resposta relacionada a incidentes críticos de segurança da informação;

VI – assessorar o Gestor de Segurança da Informação do STJ, o diretor-geral e o Secretário de Tecnologia da Informação e Comunicação na avaliação e na análise de assuntos relativos ao tratamento e resposta a incidentes de segurança da informação;

VII – colaborar na realização de auditorias e análises forenses quando solicitado pelo Secretário da STI ou superior;

VIII – comunicar à unidade encarregada de dados pessoais do STJ os incidentes de segurança da informação relacionados a dados pessoais;

IX – acompanhar o cenário mundial no contexto de segurança da informação e aplicar esse conhecimento na análise das vulnerabilidades e correções necessárias ao aprimoramento do ambiente computacional do STJ;

X – solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como:

a) tecnologia da informação;

b) segurança da informação;

c) jurídica, pesquisas judiciárias;

d) comunicação;

e) controle interno;

f) segurança institucional, entre outras;

XI - cooperar com outras equipes de tratamento e resposta a incidentes cibernéticos ou equipes equivalentes de segurança da informação de acordo com os protocolos de cooperação estabelecidos pelo Poder Judiciário;

XII - interagir com:

a) o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

b) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – DSIC/GSI/PR;

c) o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo concernente a assuntos de segurança cibernética – CTIR Gov.

Seção III
Do Funcionamento e Autonomia

Art. 5º Integram a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação servidores da Coordenadoria de Segurança da Informação e Defesa Cibernética (CSID) da Secretaria de Tecnologia da Informação e Comunicação do STJ.

§ 1º Os integrantes da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação não estão sujeitos à dedicação exclusiva, atuando mediante convocação, quando da necessidade de solução de incidentes de segurança da informação.

§ 2º Os integrantes serão nomeados por meio de portaria.

§ 3º A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação poderá convocar representantes de outras unidades do STJ para atuar no tratamento e resposta a incidentes de segurança da informação.

Art. 6º A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação atuará em consonância com as práticas, os processos e os normativos internos do Tribunal no tocante ao processo de tomada de decisão sobre as medidas a serem adotadas quanto à prevenção, ao tratamento e às respostas a incidentes de segurança da informação.

Parágrafo único. Em relação exclusivamente ao contexto de TIC, a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, sempre que possível, deverá:

I – preservar as evidências digitais do incidente;

II – coordenar as medidas de recuperação, com a finalidade de restabelecer a continuidade dos serviços interrompidos;

III – recomendar ao Gestor de Segurança da Informação do STJ os procedimentos preventivos necessários para evitar novos incidentes;

IV – atuar, de forma reativa imediatamente e preventiva, sempre que identificar incidente ou risco iminente que possa causar danos à rede, aos usuários, à imagem ou às informações corporativas do Tribunal;

V – relatar ao Gestor de Segurança da Informação do STJ e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) os incidentes críticos de segurança da informação ocorridos e as soluções adotadas, a fim de permitir a geração de estatísticas e soluções integradas.

Art. 7º São usuários dos serviços da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação:

I – os magistrados;

II – servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo;

III – estagiários;

IV – prestadores de serviço;

V – colaboradores;

VI – cidadãos atendidos diretamente ou por meio dos sistemas e serviços disponibilizados digitalmente pelo STJ.

Art. 8º Com exceção dos incidentes críticos, a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação possui plena autonomia para realizar ações necessárias na recuperação de incidentes de segurança e poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

Art. 9º Nos casos de incidentes críticos, a responsabilidade pelo direcionamento e pela condução das ações de tratamento e resposta será do Comitê de Crises Cibernéticas do STJ.

Seção IV
Dos Serviços e Canal de Comunicação

Art. 10. São serviços oferecidos pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação:

I – análise, tratamento e resposta a incidentes de segurança da informação: receber, filtrar, classificar e responder de forma reativa sempre que houver algum incidente de segurança que comprometa algum ativo de rede ou serviço de TIC no STJ, no sentido de analisar o problema, decidir sobre a melhor forma para tratar e resolver o problema com o intuito de evitar novos incidentes;

II – tratamento de artefatos maliciosos: receber e analisar arquivos e links maliciosos visando impedir sua ação dentro do STJ;

III – tratamento de vulnerabilidades: receber e analisar informações sobre vulnerabilidades em *hardware* e *software*, considerando a sua natureza e as possíveis consequências aos ativos de rede e aos serviços de TIC no STJ, visando o desenvolvimento de estratégias para a correção do problema;

IV – emissão de alertas e advertências: divulgar de forma reativa alertas e advertências imediatas diante de um incidente de segurança da informação, com o objetivo de advertir e dar orientações sobre como a comunidade deve agir diante do problema;

V – disseminação de informações relacionadas à segurança: divulgar de forma proativa alertas sobre vulnerabilidades ou problemas de segurança em TIC, cujos impactos sejam relevantes, possibilitando que a comunidade tenha conhecimento

e orientações sobre como agir e se prevenir diante de um problema.

Art. 11. A notificação de incidentes deverá ser feita por meio dos seguintes canais:

I – serviço de atendimento ao cliente – SAC do STJ por meio do telefone (61) 3319-9393 e e-mail sac@stj.jus.br (preferencialmente);

II – canal de comunicação da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação pelo e-mail etir@stj.jus.br.

Seção V
Das Disposições Finais

Art. 12. Os casos omissos serão resolvidos pelo titular da Secretaria de Tecnologia da Informação e Comunicação do Superior Tribunal de Justiça.

Art. 13. Esta instrução normativa deverá ser revisada periodicamente, em intervalos de, no máximo, três anos.

Art. 14. Esta instrução normativa entra em vigor na data de sua publicação.

MARCOS ANTONIO CAVALCANTE

Edição nº 3262 - Brasília, Disponibilização: Quinta-feira, 28 de Outubro de 2021 Publicação: Quarta-feira, 03 de Novembro de 2021
Código de Controle do Documento: 14141C51-9301-40D8-A5E5-65A128CC458E