Governo do Estado do Rio de Janeiro

Junta Comercial do Estado do Rio de Janeiro

# PORTARIA JUCERJA/SUPINF N.º 02 DE 11 DE NOVEMBRO DE 2024

**INSTITUI A EQUIPE DE TRATAMENTO E RESPOSTA À INCIDENTES COMPUTACIONAIS DA JUCERJA - ETI-JUCERJA E O MODELO DE FUNCIONAMENTO PARA APOIAR O RESPONSÁVEL PELO TRATAMENTO E RESPOSTAS A INCIDENTES DA JUCERJA.**

**O SUPERINTENDENTE DE INFORMÁTICA DA JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO – JUCERJA**, no exercício de suas competências, conforme Portaria JUCERJA nº 2233, de 07 de outubro de 2024, tendo em vista o disposto no Processo Administrativo n.º SEI-220005/002337/2024;

**CONSIDERANDO** Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021, que institui a Política da Governança de tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – PGTIC-RJ e a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – EGTIC/RJ;

**CONSIDRANDO** a Portaria JUCERJA Nº 2041 de 25 de novembro de 2022, que institui a Política de Segurança da Informação no âmbito da JUCERJA;

**CONSIDERANDO** a Portaria JUCERJA Nº 2152, de 28 de dezembro de 2024, que designa o responsável pelo tratamento e respostas a incidentes, nos termos do art. 27, do Capítulo V, da Política de Segurança da Informação da Junta Comercial do Estado do Rio de Janeiro, instituída pela Portaria JUCERJA Nº 2041/2022;

**CONSIDERANDO** a Portaria JUCERJA Nº 2153, de 28 de dezembro de 2024, que designa o Gestor de Segurança da Informação, nos termos do art. 26, do Capítulo V, da Política de Segurança da Informação da Junta Comercial do Estado do Rio de Janeiro, instituída pela Portaria JUCERJA Nº 2041/2022.

**CONSIDERANDO** a Norma Complementar no 05, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais — ETI nos órgãos e entidades da Administração Pública Federal;

**CONSIDERANDO** a Norma Complementar n° 08, de 19 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, que Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

**RESOLVE:**

**Art. 1º** Instituir a Equipe de Tratamento e Resposta à Incidentes Computacionais da Junta Comercial do Estado do Rio de Janeiro – ETI-JUCERJA, subordinada ao Responsável pelo tratamento e Respostas a Incidentes, observando as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações - POSIC da JUCERJA.

**Art. 2º** Para efeitos desta Norma, são estabelecidos os seguintes conceitos e definições:

I . **Agente responsável**: Servidor Público ocupante de cargo efetivo da JUCERJA, designado como Responsável pelo Tratamento e Resposta a Incidentes, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta à Incidentes da JUCERJA;

II. **Artefato malicioso**: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III. **Comunidade ou Público Alvo**: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

IV. **Equipe de Tratamento e Resposta à Incidentes Computacionais — ETI**: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança em redes de computadores;

V . **Incidente de segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VI. **Serviço**: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

VII. **Tratamento de Incidentes de Segurança Computacionais**: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

VIII. **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

IX. **ETI-JUCERJA**: Equipe de tratamento de incidentes computacionais da JUCERJA.

X. **GSIC** – Gestor de Segurança da Informação.

XI. **RTI**: Responsável pelo tratamento e resposta de incidentes computacionais

**Art. 3º** A Equipe de Tratamento e Resposta à Incidentes Computacionais da JUCERJA, ETI-JUCERJA, tem como missão facilitar e coordenar as atividades de tratamento e resposta à incidentes computacionais, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer a Instituição.

**Art. 4º** A amplitude das atividades pertinentes à ETI-JUCERJA incluem:

I. Todos os servidores e colaboradores que exercem suas atividades no âmbito da JUCERJA;

II. Demais equipes de resposta à incidentes de segurança da informação e comunicações da Administração Pública Estadual;

III. Órgãos Federais, Estaduais e Municipais, entidades e empresas, públicas ou privadas, que tenham contratos, acordos ou convênios com a JUCERJA para o intercâmbio de informações;

**Art. 5º** A ETI-JUCERJA adota o Modelo 1, descrito na Norma Complementar n° 05/IN01/DSIC/GSIPR, para o qual será utilizada uma Equipe de tratamento e respostas à incidentes.

§ 1º A ETI – JUCERJA será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as equipes de apoio técnico.

**Art. 6º** A ETI-JUCERJA ficará subordinada ao Responsável pelo Tratamento e Resposta a Incidentes, designado formalmente pela JUCERJA, por meio de Portaria.

§ 1º A ETI-JUCERJA será formada por servidores e/ou colaboradores da Assessoria de Redes – ASSRE e da Assessoria de Suporte – ASSUP, sem prejuízo da participação de técnicos de outras unidades da Superintendência de Informática quando convocados.

§ 2º A investigação da causa raiz de incidentes de segurança, bem como a contenção e erradicação serão coordenadas pela ETI-JUCERJA, e esta deverá ser subsidiada pelos profissionais técnicos da Superintendência de Informática, independente da subordinação ou hierarquia, objetivando clareza, inviolabilidade e veracidade para registro.

§ 3º A ETI-JUCERJA poderá ser estendida com o apoio consultivo de representantes legais de áreas especificas da Instituição, gestores, advogados, recursos humanos, controle interno, consultores técnicos, grupo de investigação ou qualquer outro que a equipe entenda ser adequado para o desenvolvimento de suas atividades.

§ 4º A omissão, subtração, destruição, desfiguração, ocultação, modificação de informações ou a não preservação de evidências de incidentes que impeçam a execução das atividades da ETI-JUCERJA serão informadas ao Gestor de Segurança da Informação, para as providências cabíveis.

**Art. 7º** Ao Gestor de Segurança da Informação – GSIC compete:

I. Revisar e aprovar estratégias de tratamento e resposta à incidentes propostos pelo Responsável pelo Tratamento de Incidentes da JUCERJA;

II. Definir acessos à internet e recursos condizentes a participação da Equipe da ETI-JUCERJA na elucidação de incidentes;

III. Aprovar a constituição, alterações na estrutura e a autonomia da ETI-JUCERJA.

IV. Estabelecer canais de comunicação com atores externos tais como Centro de Tratamento de Incidentes de Segurança de Redes de Computadores - CTIR Gov - da Administração Pública Federal - APF, Centro

de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT Br, quando for o caso, Autoridades Legais (Ministério Público, Polícia Federal, entre outros) e, outras ETIs de órgãos da APE e APF.

**Art. 8º** Ao Responsável pelo Tratamento de Incidentes da JUCERJA, responsável pela ETI-JUCERJA compete:

I. Coordenar a instituição, implementação e manutenção da infraestrutura necessária a ETI-JUCERJA;

II. Coordenar e orientar os membros da ETI-JUCERJA na gestão de incidentes;

III. Gerenciar as atividades, os procedimentos internos e distribuir as tarefas para os integrantes da ETI-JUCERJA;

IV. Coordenar o processo de capacitação e treinamento dos membros da ETI-

JUCERJA.

V. Representar a ETI-JUCERJA como apoio ao processo decisório do Gestor de Segurança da Informação, recomendando os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutir as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas);

VI. Manter registro atualizado sobre a composição da ETI-JUCERJA.

**Parágrafo único**. O exercício do encargo de que trata o caput dar-se-á sem prejuízo de suas atribuições típicas do cargo.

**Art. 9º** À Equipe da ETI-JUCERJA compete:

I. Monitorar, registrar, analisar, investigar e tratar incidentes de segurança computacionais;

Il. Emitir relatórios de notificações sobre novas ameaças e atualizações de softwares;

III. Recomendar controles aperfeiçoados ou adicionais para limitar a frequência, os danos e os impactos de futuras ocorrências de incidentes computacionais;

IV. Operacionalizar o Plano de Gestão de Incidentes de Segurança (Anexo A)

**Art. 10** A autonomia da ETI-JUCERJA é fundamentada nas recomendações da Norma Complementar n° 05 do DSIC/GSI/PR, sendo definida como compartilhada, tendo suas decisões submetidas ao Gestor de Segurança da Informação e Comunicações.

§ 1º A ETI-JUCERJA participará, através do Responsável pelo Tratamento de Incidentes, no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório.

§ 2º Uma vez tomada a decisão, a ETI-JUCERJA tem plenas condições e autonomia de adotar as medidas necessárias para a recuperação e tratamento do incidente.

§ 3º Durante um incidente de segurança computacional, se houver comprovado prejuízo à imagem institucional ou ameaça efetiva que resulte no comprometimento da segurança das informações e comunicações, a ETI-JUCERJA poderá tomar a decisão de executar as medidas necessárias para conter/erradicar o incidente, sem esperar pelo processo de tomada de decisão. Tão logo sejam adotadas as ações emergenciais, as instâncias superiores deverão ser informadas.

**Art. 11** A ETI-JUCERJA proverá, a partir de sua instituição, os seguintes serviços:

I. Tratamento e resposta de incidentes de segurança computacionais - Este serviço prevê receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail seguranca@jucerja.rj.gov.br e/ou do sistema HELP DESK (http://helpdesk/intranet.jucerja.rj.gov.br);

II. Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque ou em qualquer outra atividade maliciosa. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail seguranca@jucerja.rj.gov.br e/ou do sistema HELP DESK (http://helpdesk/intranet.jucerja.rj.gov.br);

III. Tratamento de vulnerabilidades - Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em *hardware* ou *software,* objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail seguranca@jucerja.rj.gov.br e/ou do sistema HELP DESK (http://helpdesk/intranet.jucerja.rj.gov.br);

IV. Detecção de intrusão - Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta à incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETI-JUCERJA e o CTIRGov;

V. Anúncios - Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças. Será prestado durante o horário de expediente, conforme necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Assessoria de Comunicação - ASSCOM;

Vl. Emissão de alertas e advertências - Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema. Será prestado durante o horário de expediente, conforme necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Assessoria de Comunicação - ASSCOM;

VII. Prospecção ou monitoração de novas tecnologias - Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Este serviço inclui a participação em listas de discussão sobre incidentes de segurança em redes

de computadores e o acompanhamento de notícias na mídia em geral sobre o tema;

VIII. Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores e de sistemas de informação da JUCERJA, com base em requisitos da própria organização ou em melhores prãticas de mercado.

**Art. 12** Dúvidas e casos omissos serão resolvidos pelo Gestor de Segurança da Informação - GSIC;

**Art. 13** Esta Portaria entra em vigor na data de sua publicação.

Rio de Janeiro, 11 de novembro de 2024.

**ALDO FERNANDES ÁVILA**

Superintendente de Informática

Documento assinado eletronicamente por **Aldo Fernandes Ávila**, **Superintendente**, em 11/11/2024, às 12:41, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **87239563** e o código CRC **44371C11**.

**Referência:** Processo nº SEI-220005/002337/2024 SEI nº 87239563