JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO

ATOS DO SUPERINTENDENTE

PORTARIA JUCERJA/SUPINF Nº 04 DE 23 DE MARÇO DE 2026

INSTITUI O PROCESSO DE GESTÃO DE VULNERABILIDADES CIBERNÉTICAS NO ÂMBITO DA JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO – 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 220005/001058/2026.

CONSIDERANDO a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, instituída pelo Decreto Estadual nº 48.891/2024;

CONSIDERANDO a necessidade de aprimorar a governança e os procedimentos de segurança da informação no âmbito Administração Pública Estadual, conforme diretrizes da Instrução Normativa PRODERJ/PRE nº 07, de 29 de maio de 2025;

CONSIDERANDO a necessidade de observância às diretrizes e obrigações estipuladas na Política de Segurança da Informação (POSIC) da JUCERJA, instituída pela Portaria JUCERJA nº 2.041, de 25 de novembro de 2022;

CONSIDERANDO a relevância de reduzir riscos de exploração de vulnerabilidades, preservando a confidencialidade, integridade, disponibilidade e autenticidade das informações, conforme princípios e diretrizes de segurança da informação;

CONSIDERANDO as definições relativas aos ativos críticos institucionais, conforme o PCN - Plano de Continuidade de Negócios da JUCERJA.

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, da Política de Segurança da Informação da Junta Comercial do Estado do Rio de Janeiro.

RESOLVE:

Instituir o Processo de Gestão de Vulnerabilidades Cibernéticas no âmbito da Junta Comercial do Estado do Rio de Janeiro.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria institui o Processo de Gestão de Vulnerabilidades Cibernéticas no âmbito da Junta Comercial do Estado do Rio de Janeiro – JUCERJA.

Art. 2º Esta Norma aplica-se aos responsáveis por operacionalizar as políticas e diretrizes para a gestão de vulnerabilidades, abrangendo:
I - Gestor de Segurança da Informação,
II - Responsável pelo Tratamento e Resposta a Incidentes,
III - Equipe de Resposta a Incidentes de Segurança Cibernética,
IV - Assessoria de Redes,
V - Encarregado de Dados Pessoais – DPO
VI - Servidores e colaboradores que operem, mantenham ou tenham acesso a ativos e informações da JUCERJA,

CAPÍTULO II

DOS OBJETIVOS

Art. 3º O objetivo da Gestão de Vulnerabilidades é reduzir os riscos de ataques cibernéticos decorrentes da exploração de vulnerabilidades conhecidas, constituindo-se como componente essencial para o planejamento e a implementação de controles de segurança voltados ao gerenciamento de riscos no âmbito das soluções de Tecnologia da Informação e Comunicação (TIC).

Art. 4º São metas específicas do gerenciamento de vulnerabilidades:

I – obtenção de informações confiáveis e rastreáveis sobre vulnerabilidades descobertas em soluções e ativos de TIC sob gestão, custódia ou operação da JUCERJA;

II – identificação das vulnerabilidades existentes no ambiente tecnológico da JUCERJA, incluindo, quando aplicável, ativos e serviços providos por terceiros que suportem processos e dados institucionais;

III – classificação e priorização por risco das vulnerabilidades identificadas, considerando severidade técnica, criticidade do serviço e exposição;

IV – adoção de controles de correção e/ou mitigação para reduzir impacto ou probabilidade de exploração das vulnerabilidades mais relevantes, integrando-se aos procedimentos de segurança exigidos no âmbito estadual;

V – promoção e fortalecimento da resiliência cibernética institucional, com melhoria contínua, monitoramento de resultados e conformidade com a governança estadual de privacidade e proteção de dados, quando aplicável.

CAPÍTULO III

DA PREPARAÇÃO

Art. 5º O processo de Gestão de Vulnerabilidades Cibernéticas terá escopo compatível com as capacidades operacionais das equipes de TIC da Junta Comercial do Estado do Rio de Janeiro – JUCERJA, por meio de planejamento priorizado com base em riscos identificados nos processos, serviços e ativos críticos de TIC da Autarquia, conforme descrito no PCN – Plano de Continuidade de Negócios da Instituição.

Art. 6º Integram o escopo do processo de gerenciamento de vulnerabilidades cibernéticas, observada a ordem de criticidade e priorização por risco, no mínimo:

I – vulnerabilidades expostas à internet (ativos e serviços publicamente acessíveis);

II – vulnerabilidades de fácil exploração e/ou com exploração conhecida, quando aplicável;

III – vulnerabilidades em ativos de infraestrutura crítica de TIC e serviços essenciais à continuidade institucional;

IV – vulnerabilidades massivas (de ampla incidência, com potencial de afetar grande quantidade de ativos).

Parágrafo único. A priorização deverá observar a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e os procedimentos de Segurança da Informação aplicáveis, conforme a Política de Segurança da Informação JUCERJA.

Art. 7º O inventário completo e atualizado dos ativos de informação é pré-requisito para a gestão efetiva das vulnerabilidades técnicas e deverá identificar, no mínimo:

I – ativos de hardware, software, serviços em nuvem e demais componentes tecnológicos sob gestão/custódia/operação da JUCERJA;

II – o grau de criticidade do ativo/serviço e sua vinculação a processos e serviços essenciais;
III – o responsável pela gestão do ativo/serviço;
IV – Quando aplicável, a classificação do ambiente (ex.: produção, homologação, desenvolvimento).

Parágrafo único. O inventário e o processo de vulnerabilidades deverão observar as diretrizes internas da JUCERJA, incluindo a POSIC instituída pela Portaria JUCERJA nº 2.041/2022, e as normas estaduais correlatas (quando aplicáveis).

CAPÍTULO IV

DA VERIFICAÇÃO DE VULNERABILIDADES

Art. 8º As verificações de vulnerabilidades deverão ser realizadas de forma planejada, contínua e rastreável, sob coordenação do Gestor de Segurança da Informação, observadas a propriedade intelectual de plataformas contratadas, a disponibilidade e eventual indisponibilidade de serviços institucionais, as janelas de manutenção programadas e a criticidade dos ativos, contemplando, no mínimo, as seguintes periodicidades:

Tipo de Ativo	Descrição	Criticidade	Periodicidade
Externo	Ativos expostos a Internet	Alta	Mensal
		Média	Trimestral
		Baixa	Semestral
Interno	Ativos Data Center	Alta	Pleno – Full monitoramento ativo
	Rede de dados corporativa	Alta	Quinzenal
	Estações de trabalho	Alta	Diário / sob demanda – monitoramento ativo

Os resultados das verificações deverão conter, no mínimo, identificação do ativo, evidência técnica, severidade/prioridade e recomendação de tratamento.

Art. 9º A verificação das estações de trabalho (ativos internos), presencial ou remota, quando viável, deverá ser realizada com autenticação (varredura autenticada - credentialed scan). Na impossibilidade de autenticação, poderão ser realizadas verificações não autenticadas,

devendo a limitação ser registrada e complementada por evidências adicionais (ex.: inventário de versões, coleta em end point, logs ou validação manual).

Parágrafo Único: O acesso às estações de trabalhos e ativos de TIC são irrestritos e atemporais, porém restritos às equipes autorizadas, conforme incisos I até IV, do Art. 2º.

CAPÍTULO V

DA AVALIAÇÃO E TRATAMENTO DAS VULNERABILIDADES

Art. 10 As vulnerabilidades identificadas nas verificações serão registradas em repositório centralizado para fins de acompanhamento, rastreabilidade, auditoria, e categorizadas, no mínimo, pelos seguintes critérios:

I – Utilização da métrica internacional Common Vulnerability Scoring System (CVSS), que fornece representação numérica de 0 (zero) a 10 (dez) relativa à gravidade;
II – utilização da base pública Common Vulnerabilities and Exposures (CVE) para identificação e referência das vulnerabilidades;
III – identificação quanto à existência de código, prova de conceito (PoC) ou programa explorável (exploit) associado à vulnerabilidade, bem como, outros indícios de exploração conhecida;
IV- Evidências internas de tentativa/exploração (logs, SIEM, IDS/IPS, EDR/XDR) associadas ao ambiente da JUCERJA.

Parágrafo Único: O repositório centralizado poderá ser implementado por meio de solução corporativa de gestão (ex.: plataforma de vulnerabilidades, ITSM, base de dados institucional ou solução equivalente), desde que assegure controle de acesso, integridade dos registros e trilha de auditoria.

Art. 11 As vulnerabilidades serão classificadas conforme a criticidade e priorização definidos no Art. 6º e priorizadas com base nos seguintes:

I – gravidade (severidade técnica);
II – urgência (ex.: exposição à Internet, exploração conhecida, criticidade do serviço/ativo);
III – tendência (probabilidade de aumento de exploração/propagação e impacto esperado);
IV – esforço (complexidade, dependências, janela e impacto da correção).

Parágrafo único. A priorização deverá ser compatibilizada com o planejamento das áreas responsáveis e com a disponibilidade de recursos para implementação.

Art. 12 As vulnerabilidades identificadas serão classificadas e comporão uma base de conhecimento referencial para fins de:

I – Acompanhamento do cumprimento de prazos e efetividade do tratamento;

II – Comunicação tempestiva à alta administração e às áreas responsáveis;

III – Suporte à gestão de riscos de TIC e à melhoria contínua dos controles de segurança, em consonância com as diretrizes estaduais e com a governança de privacidade e proteção de dados.

Art. 13 Na base de conhecimento referencial deverá constar, para cada vulnerabilidade, no mínimo:

I – Designação do responsável pelo ativo/serviço, quando aplicável;
II – Identificação da causa-raiz (ex.: versão desatualizada, configuração insegura);
III – Prazo para remediação, mitigação ou tratamento (SLA);

IV – Ação definida, que poderá consistir em:
a) mudança de configuração no ambiente;
b) aplicação de solução de contorno (mitigação/controle compensatório);
c) implantação de solução ou serviço de segurança;
d) aceitação o risco como exceção justificada.

Art. 14 Em relação ao tratamento das vulnerabilidades, deverão ser observados, no mínimo:

I – A integração com o processo de tratamento e resposta a incidentes de segurança da informação, incluindo a atuação do Responsável pelo Tratamento e Resposta a Incidentes, conforme a Portaria JUCERJA nº 2.041/2022;

II – A realização de testes e homologação da correção antes da publicação ou liberação em ambiente de produção, considerando risco de indisponibilidade e continuidade do serviço;

III – O cumprimento do processo de gestão de mudanças (GMUD), quando houver impacto em configurações, versões, regras de segurança, janelas de manutenção ou continuidade operacional;

IV – A observância aos normativos internos vigentes, especialmente, a POSIC da JUCERJA.

CAPÍTULO VI

DO MONITORAMENTO DE VULNERABILIDADES

Art. 15 As informações divulgadas sobre vulnerabilidades e a aplicabilidade das medidas de segurança recomendadas serão monitoradas e verificadas periodicamente pela JUCERJA, com vistas a subsidiar a avaliação de riscos, a priorização e o tratamento das vulnerabilidades.

Art. 16 São fontes de consulta preferenciais para fins de monitoramento de informações sobre vulnerabilidades:

I – comunicados, alertas e boletins de vulnerabilidades divulgados pelos fabricantes das soluções de TIC utilizadas pela JUCERJA;

II – Publicações técnicas de fabricantes e empresas especializadas em segurança da informação (ex.: boletins de segurança);

III – boletins e alertas de equipes governamentais de resposta a incidentes, com destaque para o CTIR Gov;

IV – Fontes nacionais de referência e coordenação em tratamento de incidentes, como o CERT.br;

V – Fóruns e sites especializados, quando necessários para complementar contexto técnico (PoC, indicadores, vetores), com validação crítica das informações.

Art. 17 Para análise crítica dos resultados da gestão de vulnerabilidade serão utilizados os seguintes controles:

I – Comparação dos tempos de tratamento (ex.: MTTR e cumprimento de SLA) para verificar se as vulnerabilidades foram corrigidas/mitigadas em tempo hábil;

II – Acompanhamento do nível geral de risco do ambiente tecnológico, considerando criticidade, exposição e tendência de exploração;

III – Comunicação ao Gestor de Segurança da Informação e ao Responsável pelo Tratamento e Resposta a Incidentes, bem como, à ETI-JUCERJA (Equipe de Tratamento de Incidentes**)** da JUCERJA, acerca da evolução, riscos e achados das verificações;

IV – Proposição e registro de melhorias contínuas no processo de gestão de vulnerabilidades (escopo, periodicidade, critérios de priorização, SLAs, integrações, evidências), submetendo-as à instância competente para deliberação.

CAPÍTULO VII

DOS RESPONSÁVEIS

Art. 18 Para assegurar a rastreabilidade adequada das vulnerabilidades, as responsabilidades e competências são segregadas, observados os seguintes parâmetros:

I – À Superintendência de Informática e suas unidades internas cabe a administração dos ativos e serviços de TIC institucionais (infraestrutura, sistemas, aplicações, banco de dados, segurança e correlatos), por meio dos seguintes procedimentos:

a) monitorar vulnerabilidades divulgadas por fabricantes/fornecedores das soluções utilizadas;

b) Gerenciamento de correções (*patch management*), incluindo aplicação de atualizações de segurança, upgrades e correções de configuração;

c) Registrar evidências do tratamento realizado, para fins de rastreabilidade e auditoria;

II - Ao Gestor de Segurança da Informação:

d) realizar e coordenar as verificações (internas e externas), bem como a classificação e priorização das vulnerabilidades, conforme matriz de risco adotada;

e) manter e operar o repositório centralizado de vulnerabilidades e o fluxo de acompanhamento (SLA, tickets, reincidências), garantindo vinculação ao inventário dos ativos;

f) monitorar fontes relacionadas a vulnerabilidades e medidas de tratamento (boletins oficiais/governamentais, advisors de fabricantes e fontes técnicas), registrando a rastreabilidade da origem;

g) conduzir a análise crítica dos resultados, reportar riscos e propor melhorias no processo, incluindo recomendações de controles compensatórios quando a correção imediata não for viável;

h) quando possível, utilizar evidências de telemetria e detecção (SIEM/XDR/EDR, incluindo UTMStack ou solução equivalente) como insumo para priorização e verificação de exploração.

III – À equipe de Suporte/Atendimento e Infraestrutura, cabe:

i) Operacionalizar as ações de competência do Gestor de Segurança da Informação;

j) aplicar regularmente as atualizações de segurança de sistemas operacionais em end points;

k) realizar, de forma centralizada quando possível, a atualização de aplicativos instalados em estações de trabalho, conforme política interna e planejamento de mudanças;

l) registrar evidências mínimas de execução e resultado (sucesso/erro, exceções), vinculando-as aos tickets correspondentes.

IV – Ao Responsável pelo Tratamento e Resposta a Incidentes e à Equipe de Tratamento de Incidentes, cabe:

m) priorizar o tratamento de vulnerabilidades que impactem serviços críticos e dirimir conflitos de priorização entre áreas, com decisão registrada;

n) deliberar e formalizar a designação de responsáveis quando identificadas ambiguidades quanto à titularidade ou à atribuição de responsabilidade sobre processos, sistemas, serviços ou ativos envolvidos;

o) acompanhar indicadores (SLA/MTTR/backlog) e deliberar sobre exceções e aceites de risco, com registro formal, definição de validade e indicação da autoridade competente para aprovação, nos termos do procedimento interno.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 19 Os relatórios, evidências, registros e demais documentos gerados no âmbito da Gestão de Vulnerabilidades Cibernéticas deverão ser classificados, tratados e armazenados em repositório institucional seguro, com controle de acesso, criptografia e rastreabilidade (trilha de auditoria de acesso e alterações), ficando o acesso restrito:

a) Ao Gestor de Segurança da Informação,
b) Ao Responsável pelo Tratamento e Resposta a Incidentes,
c) À Equipe de gestão segurança da Assessoria de Redes,
d) Às autoridades competentes por ocasião de auditorias técnicas internas e externas, solicitações/ordens judiciais, requerimentos de Delegacias de Polícia para fins investigativos recebidos por meio de processo administrativo autorizado pelo DPO

§ 1º Casos omissos serão submetidos à análise do Gestor de Segurança da Informação e do DPO para deliberar sobre a viabilidade do atendimento.

§ 2º A guarda, retenção e descarte desses documentos observarão os normativos internos da JUCERJA.

Art. 20 A JUCERJA poderá realizar anualmente testes de intrusão (pentest) desde que com base em planejamento que preveja rastreabilidade, escopo claro e detalhamento definido, observada a criticidade e a exposição dos ativos

§ 1º O teste de intrusão (pentest) também poderá ser realizado extraordinariamente, semestralmente, sempre que ocorrerem mudanças relevantes no ambiente, tais como:

a) nova versão de aplicação,
b) alteração de arquitetura,
c) exposição de novos serviços,
d) mudanças significativas de configuração de segurança,
e) quando houver indícios de exploração ativa,
f) mediante incidentes de segurança relevantes,
g) recomendação técnica do Responsável pelo Tratamento e Resposta a Incidentes.

§ 2º As evidências, achados e planos de correção decorrentes dos testes de intrusão deverão ser registrados em repositório oficial, vinculados aos ativos avaliados, e acompanhados até sua mitigação ou aceitação formal do risco, quando aplicável.

Art. 21 A revisão desta Portaria deverá ser realizada, preferencialmente, a cada 2(dois) anos, ou sempre que se fizer necessário, em razão de alterações tecnológicas, normativas ou organizacionais que impactem a Gestão de Vulnerabilidades Cibernéticas de segurança.

Art. 22 Esta Portaria entra em vigor na data de sua publicação, e sua operacionalização deverá ter início em até 180 (cento e oitenta) dias contados da data publicação.

ALDO FERNANDES ÁVILA

Superintendente de Informática