JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO

ATOS DO SUPERINTENDENTE

PORTARIA JUCERJA/SUPINF Nº 03 DE 16 DE MARÇO DE 2026

INSTITUI A POLÍTICA DE GESTÃO DE LOGS DE SEGURANÇA PARA AUDITORIA 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 das suas atribuições que lhe conferem a Portaria JUCERJA N. 2233 de 2024, e tendo em vista o disposto na Instrução Normativa PRODERJ/PRE Nº 02 de 28 de abril de 2022 e no Processo Administrativo n.º SEI-220005/002335/2024;

CONSIDERANDO:

- a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto nº 43.597, de 17 de maio de 2012;

- a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- o Decreto Estadual nº 48.891/2024, de 10 de janeiro de 2024, que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais no Estado do Rio de Janeiro.

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

- a Portaria JUCERJA nº 2041/2022, que institui a Política de Segurança da Informação e Comunicações da Junta Comercial do Estado do Rio de Janeiro;.

- a necessidade de padronizar, centralizar e aperfeiçoar a gestão de registros (logs) de auditoria dos recursos de tecnologia da informação da JUCERJA, como mecanismo essencial de segurança da informação, transparência, rastreabilidade e responsabilização;.

- as boas práticas de segurança da informação recomendadas pelo Center for Internet Security (CIS Controls) e demais normas técnicas aplicáveis.

R E S O L V E:

Instituir a Política de Gestão de Logs de Segurança para Auditoria no âmbito da Junta Comercial do Estado do Rio de Janeiro

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta Portaria institui a Política de Gestão de Logs de Segurança e estabelece princípios, diretrizes e responsabilidades relacionadas à gestão e à auditoria de logs de segurança no ambiente de computação e de comunicação de dados da Junta Comercial do Estado do Rio de Janeiro – JUCERJA.

Art. 2º - Para os efeitos desta Portaria, considera-se:

I – Ativos de informação – Meios de armazenamento, transmissão e processamento de informação, equipamentos necessários, sistemas utilizados, locais onde se encontram, recursos humanos que a eles têm acesso e conhecimento ou, ainda, quaisquer dados que tenham valor para a JUCERJA.

II – Ativos de informação críticos – Ativos de informação que compõem os sistemas críticos definido no item 3.3 do Plano de Continuidade de Negócios da JUCERJA – PCN e seus anexos;

III – Auditoria – Processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de

acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos institucionais;
IV – Auditoria de logs – Auditoria realizada por meio de análises em registros gerados pelos ativos de informação da JUCERJA.
V – Custodiante da informação – Indivíduo responsável pela unidade gestora que detenha responsabilidade formal sobre as informações, incluindo sua guarda, tratamento e disponibilização, nos termos da legislação aplicável;
VI – Gestão de logs – Conjunto de ações que sistematizam o planejamento, a coleta, a análise, a revisão e o armazenamento dos logs gerados pelos ativos de informação da JUCERJA.
VII – Logs – Registros detalhados de eventos em ativos de informação, tais como autenticações, acessos a dados, alterações em configurações de serviços, erros e demais eventos relevantes, com as respectivas datas e horários;
VIII – Logs de segurança – Tipo específico de log que registra eventos relacionados à segurança, sendo usado para detectar atividades maliciosas, investigar incidentes de segurança e atender a requisitos de conformidade e auditoria.
IX – Network Time Protocol – NTP – Protocolo de tempo para redes, utilizado para sincronizar a data e a hora de sistemas, equipamentos e serviços da JUCERJA; e
X – Security Information and Event Management – SIEM – Solução de gerenciamento de eventos e informações de segurança com o objetivo de detectar anomalias de comportamento por meio de correlação automatizada de eventos gerados pelos ativos de informação.

Parágrafo único. Na aplicação desta Portaria, deverão ser observados, no que couber, os conceitos constantes da legislação estadual pertinente à segurança da informação e à proteção de dados pessoais, bem como os conceitos do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Objetivos

Art. 3º - São objetivos da Política de Gestão de Logs de Segurança da Junta Comercial do Estado do Rio de Janeiro – JUCERJA:
I – Instituir princípios e responsabilidades para a gestão de registros de logs de segurança gerados pelos ativos de informação da JUCERJA; e
II – Estabelecer e manter um processo de gestão de logs que defina os requisitos de registros de segurança da JUCERJA, tratando do planejamento, da coleta, da análise e da revisão dos logs gerados pelos ativos de informação institucionais.

Abrangência

Art. 4º- As disposições desta Portaria e da regulamentação correlata aplicam-se:
I – Aos ativos informacionais da JUCERJA; e
II – Aos responsáveis pela gestão das soluções de tecnologia da informação e comunicação – TIC, aos membros da área de tecnologia, aos usuários internos e externos autorizados, bem como a provedores de serviços.

Regime de excepcionalidades

Art. 5º- Os ativos de informação críticos da JUCERJA que, por possíveis dificuldades técnicas ou por obrigações contratuais e normativas, não estejam contemplados em algum requisito desta Política, serão tratados de forma excepcional.

Parágrafo único. As excepcionalidades a esta Política deverão ser aprovadas e registradas pelo Gestor de Segurança da Informação, ouvido a Superintendência de Informática da JUCERJA, com a devida justificativa técnica e, quando couber, jurídica

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 6º - O setor responsável pela Tecnologia da Informação da Junta Comercial do Estado do Rio de Janeiro – JUCERJA (Superintendência de Informática) é responsável por elaborar, manter e fazer cumprir a Política e o Processo de Gestão de Logs de Segurança da JUCERJA.

Art. 7º - A gestão de logs de segurança é de responsabilidade conjunta:
I – Da Superintendência de Informática; e

II – Pelo Gestor de Segurança da JUCERJA.
§ 1º A Superintendência de Informática da JUCERJA é responsável por implementar a geração de logs de segurança nos ativos de informação institucionais, observadas as diretrizes desta Política e do Processo de Gestão de Registros (logs) de Auditoria.
§ 2º O Gestor de Segurança da JUCERJA, e responsável por:
I – Definir prazo de retenção adicional ao mínimo estabelecido em norma interna, de acordo com a criticidade e a relevância da informação tratada em cada solução; e
II – Definir, em conjunto com a Superintendência de Informática, as informações que deverão ser registradas nos logs de segurança, de acordo com requisitos administrativos, legais, regulatórios ou de auditoria.
§ 3º A Superintendência de Informática da JUCERJA é responsável pelas soluções de gerenciamento, correlação e validação das configurações de logs de segurança nos ativos de informação, bem como pelo acompanhamento de sua eficácia, ouvido o Encarregado de Dados Pessoais - DPO

CAPÍTULO III

DOS PRINCÍPIOS GERAIS

Art. 8º - Os ativos físicos ou virtuais, tais como servidores, equipamentos e recursos de rede da Junta Comercial do Estado do Rio de Janeiro – JUCERJA, devem ser configurados de forma sincronizada com base em uma fonte única de tempo de referência (servidores NTP institucionais ou equivalentes), de modo que os relógios de registro sejam consistentes entre si.

Art. 9º - Os processos, procedimentos e medidas técnicas relativos à gestão de logs de segurança devem ser definidos e implementados visando à proteção desses registros ao longo de todo o seu ciclo de vida, desde a geração, transmissão e armazenamento até sua exclusão segura.

Art. 10 - Os logs de segurança dos ativos informacionais que tratem de dados pessoais ou dados pessoais sensíveis devem observar as orientações contidas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e nas demais normas e regulamentações aplicáveis de proteção de dados e privacidade, inclusive as de âmbito estadual.

Art. 11 - Os logs de segurança em ativos de informação da JUCERJA devem observar o prazo de retenção mínimo de noventa dias, em prejuízo de prazos maiores que venham a ser definidos em normas internas específicas ou exigidos por legislação ou órgãos de controle.
§ 1º Os registros de acesso às aplicações da JUCERJA disponibilizadas na internet deverão, sempre que possível, ser mantidos pelo prazo mínimo de seis meses, em conformidade com a legislação aplicável e com as capacidades técnicas e de armazenamento disponíveis.
§ 2º Em casos de indisponibilidade orçamentária ou de recursos físicos e lógicos de infraestrutura, o prazo de retenção mínimo previsto no caput deverá ser priorizado para os sistemas e ativos de informação críticos da JUCERJA.

Art. 12 - O backup dos logs de segurança deverá estar incluído nas rotinas de backup dos respectivos ativos de informação ou em rotinas específicas de backup de logs, de forma a garantir a sua recuperação em caso de falhas, incidentes ou desastres.

Art. 13 - A Superintendência de Informática da JUCERJA deverá prover soluções de gestão de logs de segurança para seus ativos de informação críticos, com o objetivo de aperfeiçoar o gerenciamento desses logs, incluindo coleta centralizada, correlação, monitoramento e análise.
Parágrafo único. A Superintendência de Informática da JUCERJA, deve garantir a disponibilidade dos logs de segurança de ativos institucionais críticos e manter o controle de acesso lógico às soluções de gestão de logs de segurança, assegurando a confidencialidade, a integridade e a rastreabilidade dos registros.

CAPÍTULO IV

DAS FASES DO PROCESSO DE GESTÃO DE LOGS DE SEGURANÇA

Do planejamento

Art. 14 - Os logs de segurança dos ativos de informação da Junta Comercial do Estado do Rio de Janeiro – JUCERJA devem registrar, quando aplicável, os seguintes eventos de segurança:
I – Criação, modificação e exclusão de usuários;

II – Logo/logo de usuário;
III – Concessão ou revogação de privilégios de usuários;
IV – Modificação de perfis de acesso de usuários;
V – Alteração de senhas de usuário;
VI – Ativação ou desativação de funcionalidades;
VII – Acesso, inclusão, modificação, exclusão, impressão e *download* de informações;
VIII – Inicialização, suspensão e reinicialização de serviços; e
IX – Acoplamento e desacoplamento de dispositivos de *hardware*, principalmente mídias removíveis.
§ 1º É recomendado que os logs de segurança registrem, entre outras, as seguintes informações:
I – Identificação do ativo de informação;
II – Identificação da origem do evento;
III – Identificação única do usuário;
IV – Data e hora do evento;
V – Endereço de IP de origem do cliente, para tráfego de entrada;
VI – Endereço de IP de destino, para tráfego de saída;
VII – Ação de tratamento do dado, como consulta, inclusão, modificação ou exclusão; e
VIII – Status do resultado (sucesso, falha, erro, acesso negado, entre outros)
§ 2º Devem ser avaliados e, quando pertinentes, incluídos outros elementos úteis que possam auxiliar em investigação forense, a depender da sensibilidade da informação e da criticidade do ativo de informação envolvido.
Art. 15 - Para sistemas e serviços que tratem dados pessoais ou dados pessoais sensíveis, deve-se registrar apenas as informações estritamente necessárias, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e demais normas correlatas de proteção de dados e privacidade, garantindo a proteção e a privacidade dos titulares dos dados. A classificação, granularidade e tratamento de dados à luz da LGPD deverá ser efetuada pelo Encarregado de Dados Pessoais – DPO.
Art. 16 - O prazo de retenção adicional ao mínimo descrito no art. 11 deverá ser formalizado, pelos responsáveis, o Gestor de Segurança da Informação com a Superintendência de Informática da JUCERJA.

Da coleta

Art. 17 - A retenção dos logs de segurança deve ser configurada de acordo com os padrões mínimos definidos nesta Política e em normas internas complementares.

Art. 18 - A geração de logs de segurança deve ser implementada para todos os ativos de informação da Junta Comercial do Estado do Rio de Janeiro – JUCERJA, priorizando-se aqueles classificados como críticos, conforme classificação definida pela superintendência de Informática.

Art. 19 - Os administradores dos sistemas e serviços da JUCERJA devem configurar os ativos de informação sob sua responsabilidade para gerar e armazenar localmente os logs de segurança, observando as diretrizes de padronização, segurança e retenção previstas nesta Política.

Art. 20 - O Gestor de Segurança da JUCERJA e a Superintendência de Informática, deve implementar a coleta centralizada de logs de segurança dos ativos de informação críticos, visando à correlação, ao monitoramento e à análise integrada dos eventos de segurança.

Da análise

Art. 21 - Os logs de segurança dos ativos de informação da Junta Comercial do Estado do Rio de Janeiro – JUCERJA devem ser monitorados continuamente em busca de comportamento anômalo ou suspeito, preferencialmente utilizando solução de SIEM ou ferramenta equivalente de correlação e análise de eventos.

Art. 22 - Em caso de incidentes de segurança da informação, ou quaisquer outros eventos relevantes de segurança, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos da JUCERJA, deve preservar as evidências dos incidentes detectados.
Parágrafo único. Na impossibilidade de preservar as evidências originais, como em situações de necessidade de rápido restabelecimento dos sistemas e serviços afetados, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos da JUCERJA deve coletar e armazenar cópias dos registros e arquivos afetados pelo incidente de segurança, garantindo sua integridade e rastreabilidade.

Art. 23 - Os logs de segurança para fins de auditoria, apuração e responsabilização serão disponibilizados pela Superintendência de Informática da JUCERJA, respeitando a privacidade e o sigilo das informações, nos seguintes casos:
I – Instrução de procedimentos e processos administrativos investigativos e acusatórios conduzidos pelas unidades de correição,

controle interno ou comissão de sindicância/processo administrativo disciplinar da JUCERJA ou, quando cabível, por órgãos de controle externo do Estado do Rio de Janeiro;
II – Cumprimento de determinação judicial;
III – compartilhamento de informações solicitado por órgãos de persecução criminal, civil ou administrativa, para instrução de processos instaurados pelo órgão ou entidade solicitante, observado o devido processo legal e as normas de sigilo aplicáveis; e
IV – Solicitação formal do Comitê de Segurança da Informação, do Gestor de Segurança da Informação, do Responsável de Tratamento de Incidentes ou do Encarregado de Dados Pessoais – DPO.
Parágrafo único. Os logs de segurança de que trata o caput deverão ser disponibilizados exclusivamente ao solicitante legitimado, ficando vedada sua divulgação ou compartilhamento a terceiros não autorizados.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 24 - Os casos omissos e as dúvidas decorrentes da aplicação desta Portaria serão resolvidos pela Presidência da Junta Comercial do Estado do Rio de Janeiro – JUCERJA, ouvida, quando necessário, a Superintendência de Informática, o Gestor de Segurança da Informação.

Art. 25 - 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 logs de segurança no âmbito da JUCERJA.

Art. 26 - Esta Portaria entra em vigor na data de sua publicação.

ALDO FERNANDES ÁVILA
Superintendente de Informática