
RESOLUÇÃO CRCRJ N.º 605, DE 26 DE SETEMBRO DE 2022.

Aprova a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade do Estado do Rio de Janeiro (CRCRJ).

O CONSELHO REGIONAL DE CONTABILIDADE DO RIO DE JANEIRO, no uso de suas atribuições legais e regimentais, resolve:

CAPÍTULO I
DA POLÍTICA E DEFINIÇÕES

Art. 1º Fica instituída a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade do Estado do Rio de Janeiro (CRCRJ).

Art. 2º Para os efeitos desta Resolução, entende-se por:

I – atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

II – atividade Crítica: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III – atividade Maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema, serviço ou rede;

IV – 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 (em conformidade) à consecução dos objetivos;

V – evento de Segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas, ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

VI – fluxo de Trabalho de Incidentes: predefinição de etapas que devem ser tomadas para lidar com um tipo particular de Incidente;

VII – gerenciamento de Incidentes: processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um sistema, serviço ou rede seja restaurada tão rapidamente quando possível e que o impacto nas atividades seja minimizado;

VIII – incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação; e

IX – considera-se omissão a não observância das políticas de segurança definidas pelo CRCRJ.

CAPÍTULO II DO OBJETIVO

Art. 3º A Política de Incidentes de Segurança da Informação do CRCRJ tem por objetivos:

I – diminuir os danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência; e

II – promover a efetividade e eficácia da Política da Segurança da Informação no CRCRJ; e

III – diminuir o número total de incidentes de segurança da informação envolvendo o CRCRJ, por meio de prevenção sistemática dos eventos e eliminação de situações que permitem a ocorrência desses incidentes.

Art. 4º A Política de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação do CRCRJ e visa orientar o funcionamento do processo de gestão de incidentes de segurança digital e não digital da informação, de forma que estes sejam tratados adequadamente, reduzindo ao máximo os impactos para as atividades desenvolvidas.

CAPÍTULO III DA ABRANGÊNCIA

Art. 5º A Política de Incidentes de Segurança da Informação abrange todos os incidentes, confirmados ou sob suspeita, que envolvam o nome ou a propriedade do Conselho Regional de Contabilidade do Estado do Rio de Janeiro, bem como qualquer conselheiro, funcionário ou colaborador, no exercício da sua função ou relação com o CRCRJ.

Art. 6º A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

I – violar da Política de Controle de Ativos de Tecnologia da Informação do CRCRJ;

II – violar uma política de segurança, explícita ou implícita;

III – realizar acesso indevido ou não autorizado às instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCRJ que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

IV – realizar acesso indevido ou não autorizado aos dados, informações e documentos mantidos, tratados e controlados pelo CRCRJ que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

V – conectar dispositivo de tecnologia à rede do CRCRJ que esteja contaminado com vírus de computador detectado por mecanismo automatizado ou pessoal qualificado;

VI – violar norma de utilização ou configuração de dispositivo de tecnologia da informação, conectado ou não à rede do CRCRJ, detectada automática ou manualmente;

VII – vazar dados pessoais;

VIII – utilizar credenciais de autenticação (senhas) por indivíduo não proprietário delas ou de outrem;

IX – facilitar fluxo de comunicação de rede caracterizado como atividade maliciosa por detecção de padrão ou análise manual, ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades maliciosas;

X – omitir a comunicação de fragilidade de segurança conhecida em processo, instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pelo CRCRJ;

XI – violar direito autoral ou propriedade intelectual de qualquer natureza;

XII – realizar tentativa de fraude, bem ou malsucedida, independentemente do dano causado; e

XIII – quaisquer outros eventos que constituam violação de requisito de segurança estabelecido pela Política de Segurança da Informação do CRCRJ, tenham eles origem no próprio CRCRJ ou em grupos externos.

CAPÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I

Das competências

Art. 7º Ao Comitê Gestor de Privacidade e Proteção de Dados compete:

I – conduzir o processo de Gestão de Incidentes de Segurança da Informação;

II – investigar incidentes, levantamento, cadeia de custódia e segurança das evidências;

III – acompanhar os planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;

IV – comunicar aos líderes responsáveis; e

V – realizar as análises dos pós-incidentes, para identificação e tratamento de causas e aprimoramento de processos do CRCRJ e do próprio processo de gestão de incidentes de segurança da informação.

Art. 8º Ao Departamento de Tecnologia da Informação compete:

I – executar os procedimentos de tratamento de incidentes de segurança da informação das informações digitais definidos nesta política, observado o que dispõe o Plano de Continuidade de TI do CRCRJ, no surgimento de qualquer denúncia e ou detecção automatizada e de registrar os incidentes tratados, conforme o modelo apresentado no Anexo I – Relatório de Incidentes;

II – definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCRJ;

III – avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

IV – dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área; e

V – elaborar, anualmente, relatório estatístico do número de incidentes para fins de acompanhamento pelo CRCRJ.

Art. 9º Ao Setor de Ouvidoria e Proteção de Dados compete:

I – executar os procedimentos de tratamento de incidentes de segurança da informação das informações não digitais definidos nesta política no surgimento de qualquer denúncia e/ou detecção automatizada e de registrar os incidentes tratados;

II – definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo o CRCRJ;

III – avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos; e

IV – dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

Seção II

Das responsabilidades

Art. 10. Os líderes, ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência de acordo com os procedimentos, pré-definidos pelo Comitê Gestor de Privacidade e Proteção de Dados.

Art. 11. As responsabilidades dos conselheiros, empregados e colaboradores são:

I – devem identificar incidentes de segurança da informação quando testemunhado;

II – devem notificar qualquer evento de segurança ou fragilidade observada que possa causar: prejuízos, interrupções, mau funcionamento, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CRCRJ; e

III – devem informar imediatamente ao Departamento de Tecnologia da Informação, todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento;

§ 1º Na apuração dos incidentes de segurança da informação será considerada a vontade orientada à realização do incidente de segurança, ou seja, o elemento subjetivo que concretiza os requisitos de vulnerabilidade dos dados pessoais; e

§ 2º Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos conselheiros, empregados e colaboradores, sob o risco de violar a política de segurança digital e não digital e da informação, bem como provocar danos aos sistemas, serviços ou recursos tecnológicos digitais ou não digitais.

CAPÍTULO V DAS VIOLAÇÕES E SANÇÕES

Art. 12. Os conselheiros, empregados e colaboradores que presenciarem o descumprimento de alguma das regras acima têm o dever de denunciar tal infração.

Art. 13. O descumprimento das regras e diretrizes impostas neste documento, poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

CAPÍTULO VI DA REVISÃO E ATUALIZAÇÃO

Art. 14. A Política de Incidentes de Segurança da Informação deverá ser revista e atualizada, sempre que necessário, com vistas a se manter em sintonia com as regras de atividade, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

Art. 15. Esta Resolução entra em vigor na data de sua publicação.

CONTADOR SAMIR FERREIRA BARBOSA NEHME
Presidente

Aprovada na 1.157ª Reunião Plenária de 2022, realizada em 26 de setembro de 2022.