CRCES
CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

RESOLUÇÃO CRCES N.º 451, DE 15 DE DEZEMBRO DE 2022.

Institui a Política de Gestão de Incidentes de Segurança da Informação no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES.

O **PLENÁRIO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO,** no uso de suas atribuições legais e regimentais, nos termos do inciso XVIII, art. 11, da Resolução n.º 342/2014;

CONSIDERANDO a necessária conformidade do CRCES aos termos da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018;

CONSIDERANDO a Portaria CRCES n.º 59, de 17 de maio de 2022, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Espírito Santo;

CONSIDERANDO que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

CONSIDERANDO que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término;

R E S O L V E:

Art. 1º. Instituir a Política de Gestão de Incidentes de Segurança da Informação por meio do Manual de Gestão de Incidentes de Segurança da Informação, nos termos do Anexo desta Resolução.

Art. 2º. Esta Resolução entra em vigor na data de sua assinatura.

Contadora **Carla Cristina Tasso**
Presidente

Aprovada na 1650ª Reunião Plenária, realizada em 15 de dezembro de 2022

ANEXO

MANUAL DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Este manual estabelece a Política de Gestão de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade do Espírito Santo com o objetivo de fixar as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao seu ambiente tecnológico.

A Gestão de Incidentes de Segurança da Informação, definida nesta Política, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de Tecnologia da Informação e comunicação.

2. TERMINOLOGIA

Além das terminologias já especificadas no art. 5º da Lei Geral de Proteção de Dados Pessoais - LGPD, os seguintes termos são utilizados nesta Política de Gestão e Comunicação de Incidentes de Segurança da Informação do CRCES:

1. Artefato malicioso: 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;

2. Ativo da informação: qualquer dispositivo de *software* ou *hardware* que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCES, assim como os locais onde se encontram estes dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

3. Equipe de tratamento e resposta a incidentes em redes computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

4. Evento de segurança da informação: 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;

5. Incidente de segurança da informação: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

6. Medida de contenção: controle e/ou ação adotada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o restabelecimento do sistema/serviço afetado, mesmo que não seja em sua totalidade;

7. Medida de solução: controle e/ou ação adotada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação;

8. TI: Tecnologia da Informação;

9. Tratamento de incidentes de segurança em redes computacionais: 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;

10. Usuário: pessoa física ou jurídica que opera algum sistema informatizado do CRCES;

11. Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças.

3. DIRETRIZES

A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

Logo, esta Política abrange os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do Conselho Regional de Contabilidade do Espírito Santo, seus ativos, informações e processos de negócio, bem como aqueles que contrariam a sua Política de Segurança da Informação, e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como infração administrativa.

O CRCES providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

4. EQUIPE ENVOLVIDA

O Comitê de Segurança da Informação (CSI) tem como missão, entre outras, prover capacidade adequada para resposta e tratamento de incidentes de segurança da informação em ambiente tecnológico.

Todos os usuários do ambiente tecnológico do CRCES são público-alvo do Comitê de Segurança da Informação (CSI).

A autonomia do Comitê de Segurança da Informação (CSI) é compartilhada. A equipe recomendará, no mínimo, os procedimentos a serem executados ou as medidas de

recuperação durante um ataque e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas).

De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida à Presidência do CRCES, que decidirá em conjunto as ações a serem adotadas.

São atribuições do Comitê de Segurança da Informação (CSI) entre outras constantes em outros documentos:

I. investigar e propor ações de contenção de segurança da informação relacionadas aos ativos de tecnologia da informação;

II. receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;

III. fornecer informações aos envolvidos sobre a ocorrência e, aos usuários, orientações de prevenção de incidentes de segurança da informação;

IV. divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que posam gerar impactos nas atividades dos usuários;

V. interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, e participar de fóruns e redes nacionais e internacionais a respeito do tema.

5. PROCEDIMENTO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O procedimento de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação da gestão de segurança da informação e será composto pelas seguintes etapas:

I. detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação;

II. investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias;

III. encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações e, após seu cumprimento, o encerramento do incidente;

IV. avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas

Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, diretamente ao Encarregado pelo Tratamento de Dados Pessoais, pelo telefone ou pelo e-mail privacidade@crc-es.org.br, que a reportará ao Comitê de Segurança da Informação.

Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob risco de violar a Política de Segurança da Informação e/ou provocar danos aos serviços ou recursos tecnológicos.

A equipe de TI, responsável pelo monitoramento dos ativos, serviços e sistemas deve notificar os incidentes a eles relacionados ao Comitê de Segurança da Informação, para o devido registro e encaminhamento.

O CRCES poderá receber notificações externas sobre incidentes (ocorridos ou suspeitos) por meio de e-mail, telefone, etc, que deverão ser remetidas ao Encarregado pelo Tratamento de Dados Pessoais, para o devido encaminhamento.

O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

O Comitê de Segurança da Informação deve conduzir a investigação do incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários e evidências dos incidentes de segurança da Informação.

Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o procedimento, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, a Presidência do CRCES deverá ser comunicada, para avaliação das providências cabíveis.

O encerramento do procedimento de incidente de segurança da informação será comunicado a todas as áreas interessadas e a avaliação do procedimento de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

O desenho do procedimento de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do procedimento, serão publicados e divulgados a todos os usuários.

O procedimento será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão objeto de imediata divulgação na forma do item anterior.

6. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

A Política de Gestão 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 negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.