CRA-SC
Conselho Regional de Administração de Santa Catarina

Conselho Regional de Administração de Santa Catarina

Fiscalizar, valorizar e promover o exercício do profissional de Administração, contribuindo com o desenvolvimento do país.

Avenida Prefeito Osmar Cunha, 260 - 8º andar Edifício Royal Business Center - Bairro Centro - Florianópolis-SC - CEP 88015-100
Telefone: 0800 000 1253 - www.crasc.org.br

RESOLUÇÃO NORMATIVA CRA-SC Nº 554, DE 27 DE JUNHO DE 2024

Aprova o Plano de Resposta a Incidentes do Conselho Regional de Administração de Santa Catarina e dá outras providências.

O **PRESIDENTE DO CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SANTA CATARINA - CRA-SC**, no uso de suas atribuições que lhe são conferidas pela Lei nº 4.769, de 09 de setembro de 1965, regulamentada pelo Decreto nº 61.934, de 22 de dezembro de 1967, e o Regimento Interno do CRA-SC, aprovado pela Resolução Normativa CFA Nº 592 de 17 de dezembro de 2020, e

CONSIDERANDO a Lei n.º 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural";

CONSIDERANDO a necessidade de adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

CONSIDERANDO a Deliberação da Plenária em sessão ordinária nº 1014, realizada no dia 25 de junho de 2024;

RESOLVE:

Art. 1º Aprovar o Plano de Resposta a Incidentes do Conselho Regional de Administração de Santa Catarina, nos termos do Anexo I desta Resolução, e dar outras providências.

Art. 2º Esta Resolução Normativa entra em vigor na data da sua assinatura, revogando-se as disposições em contrário.

Adm. Djalma Henrique Hack
Presidente
CRA-SC nº 4889

ANEXO I À RESOLUÇÃO NORMATIVA CRA-SC Nº 554, DE 27 DE JUNHO DE 2024

PLANO DE RESPOSTA A INCIDENTES DO CRA-SC

CAPÍTULO I - INTRODUÇÃO

1.1 O presente Plano de Resposta a Incidentes tem como objetivo estabelecer as práticas e responsabilidades sobre a gestão de incidentes de segurança da informação e violação de dados pessoais no âmbito do CRA-SC.

1.2 O resultado esperado é o estabelecimento de condutas afins ao tratamento de informações, visando preservar e estimular princípios de integridade, confidencialidade e disponibilidade, adotando controles contra ações que possam comprometer os sistemas e recursos informatizados e estabelecendo diretrizes para todos os processos e pessoas que formam o CRA-SC.

CAPÍTULO II - DA ABRANGÊNCIA

2.1 O presente Plano aplica-se transversalmente a todas as áreas e atividades suscetíveis a ocorrência de incidentes que comprometam a confidencialidade, integridade e/ou disponibilidade de informações críticas às operações do CRA-SC, e/ou o tratamento de dados pessoais sob sua responsabilidade.

CAPÍTULO III - TERMOS E DEFINIÇÕES

I. CICLO DE VIDA DA INFORMAÇÃO: Compreende as fases de criação, coleta, classificação, armazenamento, transmissão, utilização e descarte da Informação.

II. COLABORADORES: Qualquer pessoa física ou jurídica que, por relação contratual tácita ou expressa, colabora com a consecução dos objetivos sociais do Conselho ou que tenha tido ou não acesso franqueado à Informação, independentemente de sua classificação. Nesta categoria de pessoas incluem-se, sem se limitar a estes, os empregados, estagiários, prestadores de serviços, conselheiros, representantes regionais e membros de câmaras e núcleos.

III. HARDENING: Processo de mapeamento das ameaças cibernéticas, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura.

IV. INFORMAÇÃO: Conjunto de conhecimentos e dados relacionados às atividades do CRA-SC, seus registrados, fornecedores, colaboradores e demais stakeholders, incluindo, sem limitação, de natureza comercial, técnica, financeira, pessoal, de marketing ou produto, independentemente do repositório de informação.

V. REPOSITÓRIOS DE INFORMAÇÕES: Qualquer recurso físico ou lógico utilizado no armazenamento ou manuseio da Informação. Enquadram-se nesse conceito documentos em papel, arquivos físicos,

computadores, servidores, programas de computador, bases de dados, linhas telefônicas, discos, DVD, CD, disquetes, hard-drives, pen-drives, memória flash, dentre outros.

VI. USUÁRIO: Qualquer pessoa autorizada a acessar, ler, responder, inserir, alterar ou eliminar determinada Informação.

VII. INCIDENTES DE SEGURANÇA: Qualquer evento que viabilize a quebra dos princípios de Confidencialidade, Integridade e Disponibilidade de Informações;

VIII. VIOLAÇÃO DE DADOS PESSOAIS: Qualquer acesso, aquisição, uso, modificação, divulgação perda, destruição ou dano acidental, ilegal ou não autorizado que envolva dados pessoais;

IX. COMISSÃO ESPECIAL DE GESTÃO DA LGPD: Grupo designado ao atendimento de incidentes de segurança, principalmente em casos de envolvimento de dados pessoais;

X. BOT: Código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;

XI. ENGENHARIA SOCIAL: técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;

XII. EXPURGO DE DADOS: Significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo Controlador de qualquer forma;

XIII. LOG: processo de registro de eventos relevantes num sistema computacional;

XIV. MALWARE: é um termo genérico para qualquer tipo de “malicious software” (“software malicioso”) projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos;

XV. PORTA: uma porta de conexão está sempre associada a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de e-mail que executa um serviço de SMTP usa a porta 25 do protocolo TCP;

XVI. SCRIPTS: conjunto de instruções para que uma função seja executada em determinado aplicativo; Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo CRA-SC para dar suporte na execução de suas atividades;

XVII. SNIFFING: corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um sniffer (aplicativo destinado a capturar pacotes de rede);

XVIII. SPAM: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para muitas pessoas;

XIX. SPYWARE: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

XX. VÍRUS: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

XXI. WORM: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

CAPÍTULO IV - DA PREPARAÇÃO PRÉVIA

4.1 Para a devida execução deste plano, o CRA-SC designará uma Comissão Especial de Gestão da LGPD, com membros formalmente designados e dotados de conhecimentos necessários ao gerenciamento de crises e incidentes de segurança de informações e de proteção de dados pessoais.

4.2 A Comissão deverá realizar reuniões periódicas, sendo as suas competências descritas em portaria específica.

4.3 O CRA-SC adotará instrumentos de monitoramento e comunicação de incidentes à ANPD e aos titulares de dados impactados. No mesmo sentido, divulgará em seus canais de interação com registrados e similares, informações quanto a sua política geral de privacidade e proteção de dados.

4.4 O CRA-SC adotará canais de comunicação que possibilitem que titulares de dados e/ou usuários de sistemas informatizados possam comunicar eventuais incidentes e/ou realizar solicitações.

CAPÍTULO V - DOS CRITÉRIOS GERAIS

5.1 São considerados incidentes de segurança da informação quaisquer fragilidades ou eventos adversos de segurança, sejam físicos ou lógicos, confirmados ou sob suspeita, passíveis de comprometer um ou mais princípios básicos de segurança da informação (confidencialidade, integridade e/ou disponibilidade) e, por consequência, comprometendo a consecução de objetivos do CRA-SC.

5.2 Um incidente de segurança poderá ser considerado igualmente uma violação de dados, quando ocorrer situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que envolva dados pessoais.

5.3 Todos os colaboradores devem notificar ao DPO, pelo e-mail lgpd@crasc.org.br, qualquer evento de segurança ou fragilidade observada que possam causar prejuízos, interrupções, mal funcionamentos, imprecisão ou vazamento de informação nos sistemas utilizados pela autarquia.

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

5.5 Lista-se abaixo, exemplos possíveis de incidentes de segurança da informação:

a. Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas informatizados ou das redes, bem como, estruturas físicas e lógicas associadas, que comprometa a confidencialidade, integridade e a disponibilidade do ambiente do CRA-SC;
b. Indisponibilidade do ambiente tecnológico em decorrência de ataques maliciosos, internos e/ou externos;
c. Vazamento de informações confidenciais;
d. Tentativas internas ou externas de ganhar acesso não autorizado à sistemas e dados ou, ainda, com o objetivo de comprometer o ambiente de TI;
e. Atos que violem a política de segurança da informação e/ou proteção de dados;
f. Uso de acesso não autorizado aos sistemas;
g. Utilização de dispositivos e sistemas não homologados pelo CRA-SC;
h. Modificação em sistemas sem consentimento, instruções ou conhecimento prévio de seus responsáveis;
i. Compartilhamento de credenciais de acesso lógico ou físico.

CAPÍTULO VI - DA EXECUÇÃO DO PLANO

6.1 O presente Plano de Resposta a Incidentes se desenvolverá seguindo as diretrizes abaixo:

6.1.1 ETAPA 1 - NOTIFICAÇÃO: O incidente será informado, por pessoa interna ou externa ao CRA-SC, utilizando o e-mail lgpd@crasc.org.br, sendo recebida pelo DPO, que será o acionador, o qual deverá notificar a Comissão de Gestão da LGPD para providências.

6.1.2 ETAPA 2 - TRIAGEM: A Comissão ficará responsável pela avaliação preliminar, ficando a seu cargo o descarte das notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

6.1.2.1 Durante a avaliação preliminar, a Comissão buscará informações relativas aos sistemas que foram alegadamente impactados, a criticidade do caso, quais os dados aparentes e os riscos de agravamento da situação, caso não haja resposta imediata.

6.1.2.2 Diante da avaliação preliminar, os incidentes que não envolvam sistemas online ou offline, e que seguramente não apresentam riscos aumentados pela falta de ações imediatas, serão encaminhados para trâmites regulares do CRA-SC.

6.1.2.3 No caso dos incidentes que exijam resposta imediata ou uma melhor avaliação, serão realizados os passos seguintes.

6.1.3 ETAPA 3 - AVALIAÇÃO: Será iniciada uma avaliação detalhada do incidente, identificando a unidade envolvida, a causa, endereços de IP e credenciais envolvidas, possíveis transações e

transferências de dados irregulares, métodos e vulnerabilidades exploradas, bem como determinar as ações das demais fases.

6.1.3.1 Será verificado, sobretudo, a importância do envolvimento dos profissionais especialistas nos sistemas afetados.

6.1.4 ETAPA 4 - CONTENÇÃO E ERRADICAÇÃO: Serão acionados os responsáveis pelos sistemas impactados para que se manifestem e orientem sobre os procedimentos de contenção e erradicação existentes. Esses procedimentos de contenção e erradicação visam limitar os dados e isolar os sistemas afetados para evitar novos dados decorrentes do incidente.

6.1.4.1 Nesse caso em questão, conforme necessidade e autorização, será realizado o desligamento dos sistemas por completo, ou funcionalidades específicas, incluindo a disponibilização de avisos de manutenções sempre que possível, tomando sempre o cuidado para não impactar as evidências que podem ser usadas para identificar a autoria, origem e métodos usados para quebrar a segurança.

6.1.4.2 Caso o incidente envolva máquinas virtuais, será realizada uma “cópia instantânea” das máquinas virtuais para posterior análise.

6.1.5 ETAPA 5 - RECUPERAÇÃO: O Setor envolvido tomará todas as medidas para restauração completa dos serviços ou de forma gradual (caso necessário), mediante decisão do responsável pelo sistema impactado, e transmitirá as informações para o desenvolvimento e instalação da solução adotada.

6.1.5.1 A recuperação deve seguir as medidas tomadas e identificadas na avaliação realizada, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas etc.

6.1.5.2 Caso necessário, a Comissão autorizará o prolongamento da fase de recuperação, mediante priorização dada para o devido desenvolvimento das instalações e atualizações das aplicações e do sistema operacional.

6.1.6 ETAPA 6 - COMUNICAÇÕES: Assim que encarados os procedimentos listados acima, o DPO realizará uma avaliação final junto à Comissão e fará as comunicações obrigatórias por Lei, bem como subsidiariamente, informará os encarregados de dados dos sistemas impactados.

6.1.6.1 As comunicações podem incluir agradecimentos às notificações, informações aos titulares e os relatórios formais para Agência Nacional de Proteção de Dados – ANPD.

6.1.6.2 A comunicação à ANPD será realizada utilizando o formulário específico disponível no site da Autoridade Nacional.

6.1.6.3 Os prazos e termos devem atender o art. 48 da Lei 13.709/18, observados os segredos comercial e industrial.

6.1.7 ETAPA 7 - LIÇÕES APRENDIDAS: Após contenção e resolução encaminhada, a Comissão agendará uma reunião com os envolvidos e demais colaboradores da organização, com escopo de demonstrar e discutir as lições aprendidas, erros e dificuldades encontradas, propondo melhorias para os sistemas e processos, inclusive, se for o caso, melhorias no próprio plano de resposta à incidentes.

6.1.8 ETAPA 8 - DOCUMENTAÇÕES: O incidente tratado será documentado em base de conhecimento apropriada, contendo o detalhamento das informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive, as da reunião de lições aprendidas.

CAPÍTULO VII - DAS DISPOSIÇÕES FINAIS

7.1 O presente Plano reflete as práticas adotadas pelo CRA-SC frente a cenários de exposição e/ou decorrentes de incidentes de segurança da informação e/ou tratamento de dados pessoais associados,

devendo ser revisado periodicamente, a fim de adequar-se a novas diretrizes ou políticas adotadas pela autarquia.