RESOLUÇÃO Nº 24, data da assinatura digital

Aprova o Plano de Respostas de Incidentes - LGPD do Corpo de Bombeiros Militar de Santa Catarina.

O COMANDANTE-GERAL DO CORPO DE BOMBEIROS MILITAR DO ESTADO DE SANTA CATARINA, no uso de suas atribuições, alicerçado na Lei Complementar n° 724, de 18 de julho de 2018 e no Decreto nº 1.328, de 14 de junho de 2021,

RESOLVE:

Art. 1º Aprovar o Plano de Respostas de Incidentes - LGPD do Corpo de Bombeiros Militar de Santa Catarina.

Art. 2º Publicar esta Resolução em Boletim do Corpo de Bombeiros Militar.

Art. 3º Esta Resolução entra em vigor na data de sua assinatura.

Florianópolis, data da assinatura digital

Coronel BM FABIANO DE SOUZA
Comandante-Geral do CBMSC
(assinado digitalmente)

PLANO DE RESPOSTA DE INCIDENTES - LGPD

1. OBJETIVO E INFORMAÇÕES

a) Trata-se do plano de resposta de incidentes, relacionados a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e tem como objetivo definir os procedimentos a serem adotados pelo Corpo de Bombeiros Militar de Santa Catarina (CBMSC) caso este venha estar contido em um incidente envolvendo vazamento de dados pessoais.
b) Execução: Encarregado pelo tratamento de dados pessoais do CBMSC.
c) Versão: primeira (V1).

2. FUNDAMENTAÇÃO LEGAL

a) Constituição da República Federativa do Brasil de 1988, Art. 5º;
b) Emenda Constitucional nº 115/2022 elenca a proteção de dados pessoais como garantia fundamental;
c) Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais;
d) Decreto Estadual nº 1.184, de 1º de março de 2021 - Dispõe sobre proposições gerais objetivando a implementação da Lei federal no 13.709, de 2018, no âmbito do Poder Executivo Estadual;
e) Portaria nº 358-2020-CBMSC - Política de Proteção de Dados do Corpo de Bombeiros Militar de Santa Catarina; e
f) Guia de Resposta a Incidentes de Segurança - Versão 1.0 Florianópolis, fevereiro de 2022 – Secretaria de Estado da Administração.

3. ENTRADA

Identificação de um incidente envolvendo dados pessoais tratados pelo CBMSC e a notificação da Corporação através de Nota eletrônica (e-mail) – lgpd@cbm.sc.gov.br ou pelo sistema disponível no site https://www.sc.gov.br/servicos/detalhe/solicitar-atendimento-lgpd, ou pelo telefone (48) 3665-7664 ou ainda por meio do Sistema de Gestão de Processos Eletrônicos (SGPE) - CBMSC/LGPD-DPO.

4. DETALHAMENTO DE ATIVIDADE

4.1 Identificação do incidente

a) A identificação de um incidente envolvendo dados pessoais tratados pelo CBMSC pode ser realizada por qualquer pessoa física ou jurídica, a qual poderá notificar a Corporação, preferencialmente pelo e-mail lgpd@cbm.sc.gov.br ou pelo sistema disponível no site https://www.sc.gov.br/servicos/detalhe/solicitar-atendimento-lgpd, ou pelo telefone (48) 3665-7664 ou ainda se dirigindo a qualquer unidade do CBMSC e relatando o fato a um Bombeiro Militar, o qual tem o dever de formalizar a referida demanda ao encarregado pelo tratamento de dados pessoais no CBMSC, através do e-mail lgpd@cbm.sc.gov.br, ou por meio do Sistema de Gestão de Processos Eletrônicos (SGPE) - CBMSC/LGPD-DPO ou por qualquer outro canal efetivo de comunicação que transmita a informação de modo imediato.

b) Ao tomar conhecimento de um incidente envolvendo dados pessoais tratados pelo CBMSC o encarregado pelo tratamento de dados pessoais no CBMSC deve realizar os procedimentos elencados abaixo, respectivamente:

1. avaliar internamente o incidente para obter informações iniciais sobre o impacto do ocorrido, tais como: fonte, categoria, quantidade de titulares e de dados pessoais afetados, categoria e quantidade de dados afetados, consequências do incidente para os titulares e para a corporação, criticidade e probabilidade, e preservação de todas as evidências do incidente coletadas;
2. comunicar o Controlador (Comandante-Geral do CBMSC) sobre o incidente para que este determine as medidas necessárias para contenção do incidente, nos termos da LGPD; e
3. comunicar o Operador (Diretor responsável pelo sistema envolvido) sobre o incidente para que este tome as medidas adequadas à contenção do incidente (ver 4.2).

4.2 Contenção do incidente

a) Confirmado o incidente envolvendo dados pessoais tratados pelo CBMSC, ou mesmo que não confirmado mas existindo fundamentada suspeita, o Operador deve:
1. retirar o acesso do sistema de rede externa de internet (retirar do ar);
2. aplicar medidas tecnológicas para reforço da segurança dos dados pessoais tratados pelo CBMSC; e
3. conter o acesso não autorizado aos dados pessoais tratados pelo CBMSC.

4.3 Confirmação do incidente

a) A confirmação de um incidente envolvendo dados pessoais tratados pelo CBMSC se utilizará, quando necessário, de toda a estrutura disponível na corporação e da estrutura administrativa do Estado de Santa Catarina.

b) O Encarregado pelo tratamento de dados pessoais no CBMSC deve consultar e comunicar:
1. o Grupo de Trabalho Interno de implementação da LGPD no CBMSC;
2. os envolvidos no incidente relacionado aos dados tratados pelo CBMSC; e
3. o Comitê Gestor de Proteção de Dados Pessoais – CGPD/SC.

c) O Controlador (Comandante-Geral do CBMSC) deve realizar as seguintes ações:
1. comunicar o incidente ao Governador do Estado;
2. registrar um Boletim de Ocorrência na Polícia Civil, caso este incidente tenha ocorrido por ataques externos; e
3. determinar a apuração legal cabível pela Corregedoria do CBMSC caso o referido vazamento tenha ocorrido por dolo ou culpa de agentes internos da corporação.

4.4 Notificação do incidente à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados pessoais envolvidos

a) A LGPD prevê em seu art. 48, que, em caso de ocorrência de incidente, o controlador deve notificar tanto o titular como a ANPD em um prazo razoável, exceto nos casos em que a violação não apresente um risco de relevância aos direitos e liberdades dos indivíduos, como, por exemplo, quando os dados forem anonimizados ou criptografados.

b) O Controlador (Comandante-Geral do CBMSC) deve determinar:
1. ao encarregado pelo tratamento de dados pessoais no CBMSC que este comunique a ANPD, nos termos previstos da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e nos termos previstos nas resoluções e regulamentos da ANPD, o incidente ocorrido envolvendo os dados pessoais tratados pelo CBMSC;
2. ao Chefe do Centro de Comunicação Social do CBMSC que este publique na página Oficial do CBMSC a informação sobre o incidente envolvendo dados pessoais tratados pelo CBMSC, bem

como medidas de segurança a serem adotadas pelos titulares de dados pessoais usuários do referido sistema afetado; e
3. ao Operador do sistema afetado, que havendo o cadastro de e-mail dos titulares de dados afetados pelo incidente, este formalize uma comunicação eletrônica informando sobre o incidente, e deve sugerir medidas de segurança a serem adotadas pelo respectivo titular de dados pessoais para mitigação de possíveis danos.

4.5 Relatório final do incidente

a) O relatório deve ser emitido pelo Operador do sistema afetado pelo incidente, sob supervisão do Encarregado pelo tratamento de dados pessoais no CBMSC e homologado pelo Controlador (Comandante-Geral do CBMSC), contendo todas as evidências e ações realizadas para o tratamento do incidente que deve

b) O relatório final contendo os tipos de dados e a quantidade de titulares afetados deve ser acompanhado de informações técnicas de tratamento de dados pessoais, as quais permitirão avaliar extensão e adequação de medidas para incidentes futuros.

4.6 Reformulação e retomada do serviço

a) Após a adoção de todas medidas necessárias relacionadas às correções dos fatores que ocasionaram o incidente envolvendo dados pessoais tratados pelo CBMSC, bem como a adoção de medidas de segurança visando a preservação da segurança da informação, o Operador do sistema afetado pelo incidente, deve apresentar todas as medidas realizadas ao Controlador (Comandante-Geral do CBMSC), a fim de obter a autorização para restabelecer o sistema na rede de internet e disponibilizar aos usuários externos.

5. SAÍDAS

Elaboração do relatório final do incidente e reformulação e retomada do serviço.

6 ANEXO

a) Anexo A - Funções previstas na LGPD.
b) Anexo B - Fluxograma.
c) Anexo C - Checklist para verificação do tratamento de incidentes

7 PUBLICAÇÃO

a) SGPe: Processo CBMSC 00023769/2023.

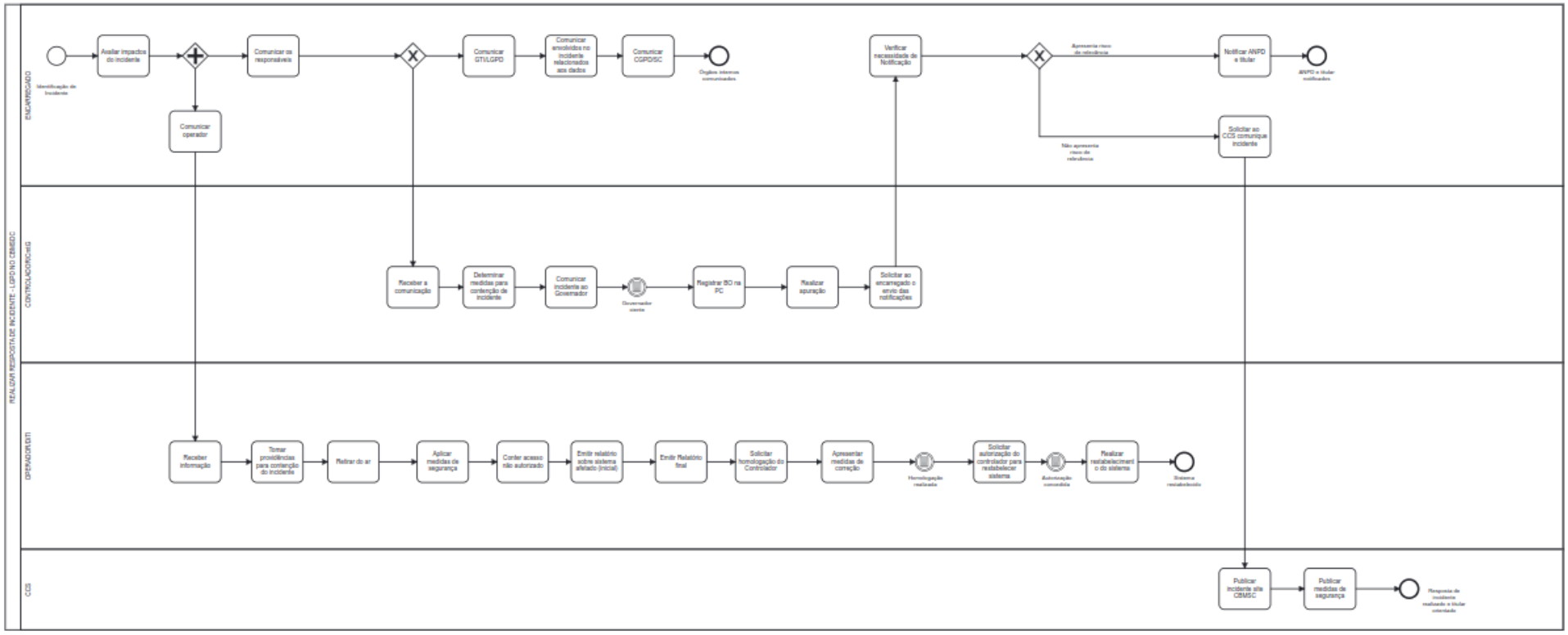
Florianópolis, data da assinatura digital

Coronel BM FABIANO DE SOUZA
Comandante-Geral do CBMSC
(assinado digitalmente)

ANEXO A

PAPEL	PESSOA DESIGNADA	CONTATO
Controlador	Comandante-Geral do CBMSC	gabinete@cbm.sc.gov.br
Operador	Diretor da Diretoria ou Agência responsável pelo sistema. Quando não houver uma Diretoria responsável pelo sistema o operador será a Divisão de Tecnologia da Informação.	ditich@cbm.sc.gov.br aisach@cbm.sc.gov.br diedir@cbm.sc.gov.br dscidir@cbm.sc.gov.br dpdir@cbm.sc.gov.br dlfdir@cbm.sc.gov.br
Encarregado de dados pessoais	Ouvidor-Geral do CBMSC	lgpd@cbm.sc.gov.br SGPE: CBMSC/LGPD-DPO
Grupo de Trabalho - GTI	I - Chefe Da Agência de Integração de Serviços Auxiliares (AISA); II - Ouvidor-Geral do CBMSC (encarregado da LGPD); III - Chefe da Divisão de Tecnologia da Informação (DiTI); IV - Secretário do Estado-Maior Geral do CBMSC; V - Chefe do Centro de Comunicação Social (CCS); VI - Chefe da Assessoria Jurídica (Ass Jur); VII - Chefe do Centro de Pesquisa e Inovação (DSCI); VIII - Chefe do Centro de Justiça e Disciplina (DP); IX - Chefe do Centro de Convênios (CCV); e X - Chefe do Centro de Avaliação e Estatísticas (CAE/DICAE/DIE).	SGPE: CBMSC/LGPD-GTI
Jurídico	Assessoria Jurídica do CBMSC	assjur@cbm.sc.gov.br
Relacionamento e atendimento	Ouvidoria do CBMSC	http://ouvidoria.sc.gov.br/

ANEXO B
Fluxograma



ANEXO C

CHECKLIST PARA VERIFICAÇÃO DO TRATAMENTO DE INCIDENTES

	Ação	Realizado?
	Detecção e análise	
1.	Determinar se ocorreu um incidente	
1.1	Analisar os precursores e os indicadores	
1.2	Buscar por informações correlatas	
1.3	Realizar pesquisa do incidente (via mecanismos de busca e bases de conhecimento)	
1.4	Documentar, investigar e reunir de evidências assim que a equipe identificar a ocorrência do incidente	
2.	Priorizar o tratamento com base em sua relevância (impacto de negócio, impacto de informação e recuperabilidade)	
3.	Comunicar o incidente às equipes internas envolvidas e, quando necessário, aos atores externos	
	Contenção, erradicação e recuperação	
4.	Coletar, preservar, proteger e documentar as evidências	
5.	Conter o incidente	
6.	Erradicar o incidente	
6.1	Identificar e mitigar todas as vulnerabilidades exploradas	
6.2	Remover malware, materiais impróprios e outros componentes	
6.3	Se mais hosts afetados forem descobertos (por exemplo, novas infecções por malware), repetir as etapas de detecção e análise (1.1, 1.2) para identificar todos os outros hosts afetados, para então conter (5) e erradicar (6) o incidente em tais hosts	
7.7.	Recuperar-se do incidente	
7.1	Retornar os sistemas afetados ao estado operacional	
7.2	Confirmar se os sistemas afetados estão funcionando normalmente	
7.3	Se necessário, implementar monitoração adicional para encontrar futuras atividades relacionadas	
	Atividades pós-incidente	
8.	Criar o relatório de acompanhamento	
9.	Realizar uma reunião de lições aprendidas (tal reunião é obrigatória para incidentes graves e opcional para os demais incidentes)	

Fonte: Plano de Resposta a Incidentes de Segurança 1ª versão 2022 – SEA/SC

Assinaturas do documento

Código para verificação: **9IR81IC2**

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

FABIANO DE SOUZA (CPF: 021.XXX.519-XX) em 15/11/2023 às 13:11:19
Emitido por: "SGP-e", emitido em 20/02/2019 - 10:52:47 e válido até 20/02/2119 - 10:52:47.
(Assinatura do sistema)

Para verificar a autenticidade desta cópia, acesse o link https://portal.sgpe.sea.sc.gov.br/portal-externo/conferencia-documento/Q0JNU0NfOTk5Ml8wMDAyMzc2OV8yMzk0NF8yMDIzXzlJUjgxSUMy ou o site https://portal.sgpe.sea.sc.gov.br/portal-externo e informe o processo **CBMSC 00023769/2023** e o código **9IR81IC2** ou aponte a câmera para o QR Code presente nesta página para realizar a conferência.