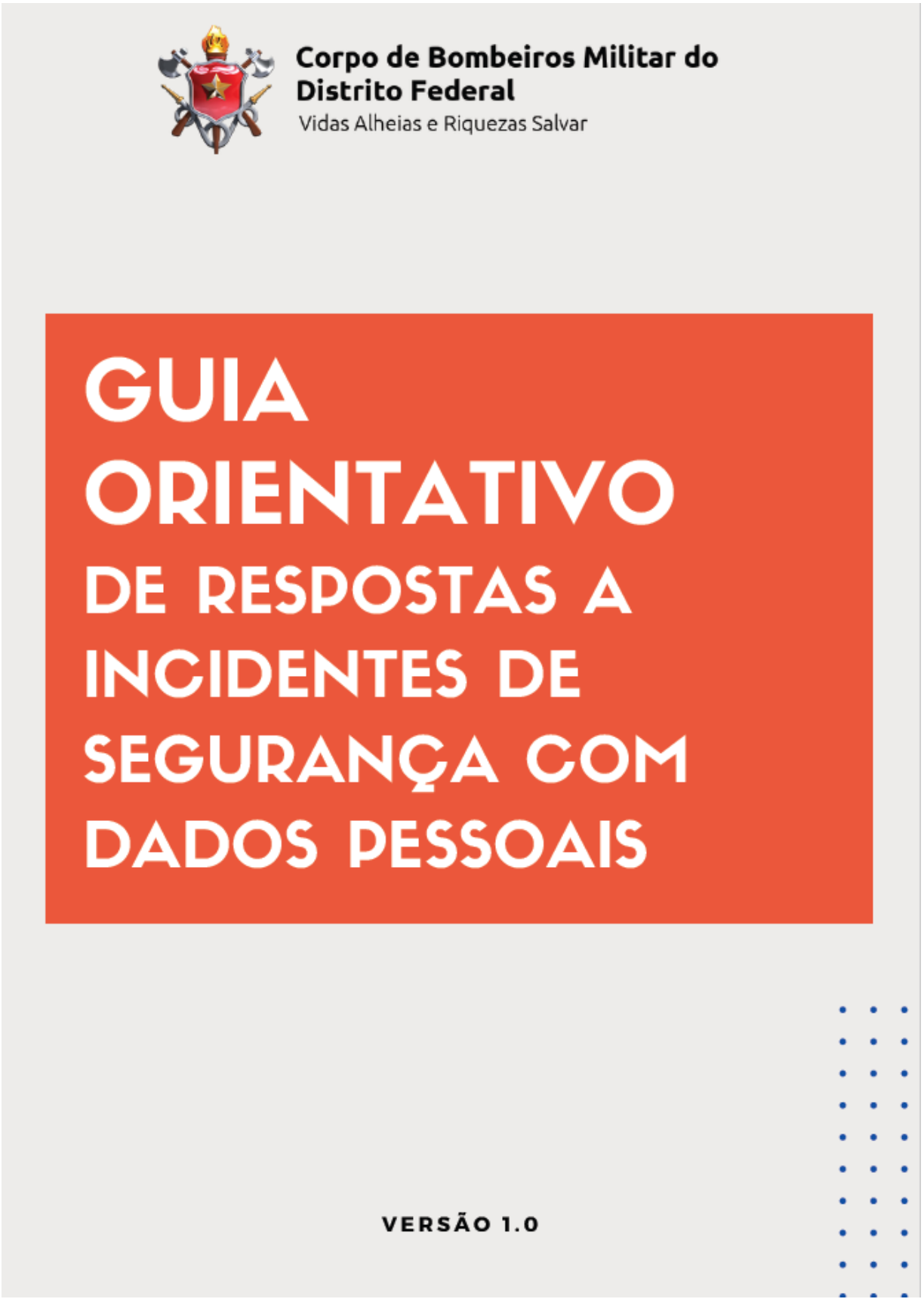
ANEXO 6

VOLTAR



APROVAÇÃO:

CONTROLADOR DO CBMDF:

- ENCARREGADO SETORIAL DO CBMDF EM FACE À LEI FEDERAL Nº 13.709, DE 14 DE AGOSTO DE 2018 - GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD);
- PRESIDENTE DA COMISSÃO PARA PROPOSIÇÃO DE PROJETO DE ADEQUAÇÃO DO CBMDF À LGPD

ELABORAÇÃO E ORGANIZAÇÃO:

CONSULTORES DA COMISSÃO PARA PROPOSIÇÃO DE PROJETO DE ADEQUAÇÃO DO CBMDF À LEI FEDERAL Nº 13.709, DE 14 DE AGOSTO DE 2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD):

- TC RRM/PTTC BENUR WANDERLEY MIRANDA DA SILVA
- MAJ QOBM/COMPL ARNALDO ALVES DE ALVARENGA
- CAP QOBM/COMPL BRUNA DE MELO COELHO
- CAP QOBM/INTD ERLERANDRO LOPES DA SILVA

SUMÁRIO

03 Introdução

06 Termos e Definições

12 Incidentes de segurança com dados pessoais

14 Fluxo de respostas a incidentes de segurança com dados pessoais

29 Referência Bibliográfica

31 Formulário

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes sólidas para a proteção dos dados pessoais no Brasil. Desde a sua promulgação, as organizações públicas e privadas têm enfrentado o desafio de adequar suas práticas de tratamento de dados pessoais.

Dado o grande volume de dados que o Corpo de Bombeiros Militar do Distrito Federal - CBMDF lida e a importância crucial de seu papel institucional na prestação de serviços públicos, é fundamental que a Corporação reconheça a possibilidade concreta de ocorrência de incidentes de segurança. Esses incidentes devem ser prevenidos por meio da implementação de medidas de proteção e prevenção adequadas.

Nesse sentido, a conformidade com a LGPD vai além da aplicação de tecnologias e padrões de segurança. Envolve também a elaboração, manutenção e revisão de documentos que não apenas garantam a conformidade com a legislação, mas também aprimoram a organização e a eficiência dos processos internos.

De acordo com a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), um incidente de segurança com dados pessoais diz respeito a "qualquer evento adverso confirmado, relacionado à violação na segurança de dados

pessoais, tais como acesso não autorizado, acidental ou ilícito, que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais".

Para evitar ou minimizar os riscos de incidentes de segurança, os agentes de tratamento devem adotar medidas preventivas, de modo a proteger os dados pessoais. Nessa conformidade, o art. 20 da Portaria 2, de 11 de fevereiro de 2022, que estabeleceu a Política de Proteção de Dados Pessoais – PPDP no âmbito do CBMDF, dispõe que:

> O CBMDF deve adotar boas práticas de governança capazes de inspirar comportamentos adequados e de mitigar os riscos de comprometimento de dados pessoais.

Nesse contexto, o presente **"Guia Orientativo de Respostas a Incidentes de Segurança com Dados Pessoais no âmbito do CBMDF"** visa informar a todos os militares, servidores, terceirizados e demais colaboradores sobre as medidas a serem tomadas em situações de emergência ou de eventos que possam colocar em risco a segurança dos dados pessoais custodiados pela Corporação. Dessa forma Pretende-se:

- Assegurar resposta rápidas e efetivas aos incidentes de segurança com dados pessoais no âmbito do CBMDF;
- Documentar e resguardar evidências que possam prevenir possíveis incidentes;
- Estabelecer diretrizes necessárias para facilitar a comunicação apropriada e tempestiva com a Autoridade Nacional de Proteção de Dados, quando necessário e sob a égide da transparência, em estrita observância à Lei Federal nº 13.709, de 14 de agosto de 2018 e às Leis de Acesso à Informação de âmbito Federal e Distrital, quais sejam a Lei nº 12.527, de 18 de novembro de 2011 e Lei nº 4.990, de 12 de dezembro de 2012.

05

TERMOS E DEFINIÇÕES

De modo a impulsionar o melhor entendimento e compreensão deste Guia Orientativo, serão adotadas as seguintes conceituações constantes da Lei Federal nº 13.709, de 14 de agosto de 2018 e do Decreto Distrital nº 42.036, de 27 de abril de 2021:

- **Agentes de tratamento**: de acordo com a LGPD, são agentes de tratamento:
  - CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No CBMDF, o Controlador é o(a) Comandante-geral;
  - OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No CBMDF, segundo sua Política de Proteção de Dados Pessoais, o Operador será qualquer militar colaborador que exerça atividade de tratamento de dados pessoais na Corporação.

- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

- **Banco de Dados Pessoais (BDP):** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

- **Dado Pessoal (DP):** informação relacionada a pessoa natural identificada ou identificável;

- **Dado Pessoal Sensível (DPS):** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

- **Dado Pessoal Anonimizado (DPA):** dado relativo a titular que, por meio de tratamento específico, mediante a utilização de meios técnicos razoáveis e disponíveis, não possa ser identificado;

- **Dado Pessoal Pseudoanonimizado (DPP):** dado relativo a titular que, por meio de tratamento específico, mediante a utilização de meios técnicos razoáveis e disponíveis, perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

- **Encarregado ou Data Privacy Officer (DPO):** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No CBMDF, o Encarregado é o Controlador.

- **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;

- **Incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

- **Incidente de segurança com dados pessoais:** qualquer evento adverso, confirmado ou sob suspeita,

- relacionado à violação de dados pessoais, por meio de acesso não autorizado, acidental ou ilícito, que resulte em vazamento, destruição, perda, alteração ou qualquer forma de tratamento inadequado, com a manifesta capacidade de pôr em risco os direitos e as liberdades dos respectivos titulares;

- ***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, sendo que existem muitos tipos de *malware*, e cada um funciona de maneira diferente na busca de seus objetivos;

- **Sistemas:** hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela Corporação para propiciar suporte na execução de suas atividades meio ou fim;

- ***Spam:*** termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- **Tratamento de Dados Pessoais (TDP):** qualquer operação ou conjunto de operações efetuadas sobre os dados pessoais, por meios automatizados ou não, incluindo, mas não se limitando a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração, gravação, organização, estruturação, alteração, divulgação, cópia, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição, anonimização e pseudoanonimização;

- ***Trojan* (Cavalo de Troia):** programa que, além de executar as funções para as quais foi aparentemente projetados, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

- **Vazamento de dados:** qualquer quebra de sigilo que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados, de forma não autorizada;

- **Violação de privacidade:** qualquer quebra protocolar de acesso em relação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita de dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

- **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.

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Incidentes de segurança com dados pessoais são eventos adversos que comprometem a privacidade, a integridade ou a disponibilidade de dados pessoais.

Podem decorrer tanto de ações acidentais, como o envio de informações para o destinatário incorreto, quanto de ações intencionais, como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados. Em geral, tais ações resultam em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estejam armazenados.

Os incidentes de segurança não se limitam pois, a vazamentos de informações ou a violações de confidencialidade. Eles incluem também a perda ou a indisponibilidade de acesso aos dados pessoais.

Como exemplos, podemos citar o sequestro de dados (*ransomware*), os acessos não autorizados a sistemas de armazenamento e a divulgação não planejada de dados pessoais

É importante saber que nem todo problema com a segurança da informação envolve dados pessoais! Nesse sentido, se os dados envolvidos estiverem anonimizados ou não puderem identificar indivíduos específicos, não haverá a necessidade de comunicação à ANPD.

Além disso, é preciso salientar que **uma mera vulnerabilidade em um sistema de informação não significa necessariamente um incidente de segurança com dados pessoais.** No entanto, tais circunstâncias merecem atenção, pois a exploração da referida vulnerabilidade pode resultar em um incidente.

FLUXO DE RESPOSTAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Conforme o art. 46 da LGPD "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".

Tais medidas de segurança deverão ser observadas durante todo o tratamento de dados pessoais, ou seja, ao longo de todas as operações realizadas desde a concepção até o armazenamento ou eliminação. Ressalta-se a necessidade de observação da legislação arquivística, no que couber.

De um modo geral, e adotando-se os parâmetros da ANPD, o Corpo de Bombeiros Militar do Distrito Federal deverá realizar os seguintes procedimentos em caso de incidente que coloque em risco a segurança de dados pessoais:

Identificação

O processo de resposta a um incidente de segurança com dados inicia-se com a identificação do incidente.

Conforme já abordado neste guia, esse tipo de incidente refere-se a qualquer evento adverso, confirmado ou suspeito, relacionado com a violação de dados pessoais. Isso inclui acessos não autorizados, acidentais ou ilícitos que resultem na destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado de dados, que tenham o potencial de ameaçar os direitos e liberdades dos titulares desses dados pessoais.

Um incidente pode ser identificado por meio de diversas situações, como a interrupção não planejada de um serviço de TI, o recebimento de e-mails contendo links suspeitos ou código malicioso que permite ao invasor controlar remotamente o dispositivo afetado, bem como outras ocorrências suspeitas, como vírus, ataques cibernéticos e outros.

Ressalta-se, pois, que os incidentes de segurança não se restringem a dados armazenados em mídias digitais, podendo recair ainda sobre dados armazenados em suportes como documentos físicos.

Notificação do incidente

Qualquer pessoa, seja bombeiro militar ou não, que venha a identificar indícios de incidente de segurança com dados pessoais tratados pelo CBMDF, no exercício de suas funções, poderá notificar o Encarregado Setorial de Dados da Corporação.

Se militar, a comunicação deverá ser realizada por meio do preenchimento do "FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS" que será disponibilizado junto ao Sistema INOVA/CBMDF.

Em caso de usuário externo, ou da impossibilidade de utilização do Sistema Inova, a notificação deverá ser realizada, preferencialmente, por meio do canal de comunicação com a Ouvidoria. Há ainda a viabilidade da comunicação ser feita pessoalmente, por meio do telefone da Ouvidoria, ou por quaisquer mecanismos de comunicação direta que venham a ser criados.

Ao se registrar uma notificação de incidente de segurança com dados pessoais, sugere-se, sempre que possível, inserir as seguintes informações para controle e armazenamento:

- Dados do responsável pela comunicação do incidente: e-mail, telefone ou outro contato disponível;
- Origem do incidente: unidade, setor ou organização à qual o dispositivo ou o processo que originou o incidente pertence;
- Registro do tempo da ocorrência do incidente: data e hora na qual o incidente foi identificado;
- Local onde se originou o incidente;
- Descrição do incidente: breve descrição do incidente, identificando o tipo de incidente, quais tipos de dados estão envolvidos, se há alguma motivação aparente, ou outras características relevantes;

- Informar se os dados pessoais envolvidos no incidente são sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- Logs ou evidências: anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente;

A Ouvidoria da Corporação ao recepcionar a notificação deverá submetê-la imediatamente ao Controlador do CBMDF, na qualidade de Encarregado pelo Tratamento de Dados Pessoais junto ao(a) Encarregado Governamental no âmbito do Distrito Federal e à Autoridade Nacional de Proteção de Dados no âmbito Federal, com vistas à adoção das correlatas providências legais.

Registro

A notificação de incidente de segurança deverá ser registrada em base de conhecimento apropriada, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicação do incidente ao(à) Comandante-Geral

O Encarregado pelo Tratamento de Dados Pessoais no âmbito do CBMDF, comunicará imediatamente ao(à) Comandante-Geral do CBMDF, enquanto representante do Controlador (nos termos da Portaria nº 02, de 11 de fevereiro de 2022), por relato prévio, acerca do fato e das providências em curso para análise do possível incidente de segurança. As informações levantadas subsidiarão, quando necessário, a notificação à Autoridade Nacional de Proteção de Dados, nos termos do art. 48 da LGPD.

Triagem e Classificação

O Encarregado Setorial do CBMDF deverá contatar o Dirigente da Organização Bombeiro Militar envolvida com o incidente de segurança, bem como o Diretor de Tecnologia da Informação e Comunicação, nos casos de necessidade de maiores suportes técnicos de TI, a fim de obter informações preliminares. Objetiva-se, pois, verificar se o evento se trata de fato de um incidente de segurança com dados pessoais, descartando-se as notificações improcedentes.

Caso se confirme o incidente de segurança com dados pessoais, o Encarregado deverá designar, no prazo não superior a 24 (vinte e quatro) horas úteis, um oficial responsável por avaliar de forma mais detalhada o evento.

Objetiva-se nessa avaliação reunir o máximo de informações sobre o evento, a exemplo de:

a) Qual vulnerabilidade foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b) Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

c) Categoria de dados pessoais: dados sensíveis, dados pessoais de crianças e adolescentes.

d) Extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

e) Avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos titulares.

f) Avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem do CBMDF em âmbito nacional e internacional, prejuízo à Corporação em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas.

Quanto à criticidade e impacto envolvido, deve-se classificar o incidente de acordo com os seguintes critérios:

(I) ALTO (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o CBMDF;

(II) MÉDIO (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao CBMDF; e

(III) BAIXO (impacto mínimo): possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho institucional detalhado.

Ressalta-se que, durante a avaliação, devem ser preservadas todas as evidências possíveis. Além disso, deve-se documentar todas as medidas que foram adotadas desde a ciência do incidente, a fim de que se possa apresentar, quando necessário, todas as ações realizadas para compreender e reduzir os efeitos do incidente ocorrido.

Comunicação do incidente ao Encarregado Governamental

Constatado o incidente de segurança com dados pessoais, o Encarregado Setorial de Dados Pessoais do CBMDF deverá comunicar o Encarregado Governamental, nos termos do Decreto Distrital nº 42.036, de 27 de abril de 2021, acerca do incidente de segurança identificado.

Comunicação do incidente à Autoridade Nacional de Proteção de Dados e aos titulares dos dados pessoais

O(a) Comandante-Geral do CBMDF, na qualidade de representante do Controlador(a) de Dados Pessoais, e nos termos do artigo 48 da LGPD, deverá comunicar à ANPD e ao titular de dados pessoais quanto às providências adotadas acerca do incidente, sobretudo nos casos de risco

ou dano relevante aos titulares, mencionando no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;
- os motivos da morosidade, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD estipula o prazo de dois dias úteis para comunicação do incidente de segurança a proteção de dados.

A comunicação aos titulares dos dados pessoais deve ser feita individualmente, sempre que possível. Se, devido à natureza do incidente, não for possível identificar individualmente os titulares afetados, todos os indivíduos presentes na base de dados comprometida devem ser informados.

Contenção, Erradicação e Recuperação

Após a análise do incidente de segurança com dados pessoais, deverão ser realizadas ações para mitigação do evento.

O objetivo das medidas de contenção é impedir que o cenário não seja ampliado. Dessa forma, deve-se, dentre outras ações:

- Desativar o sistema comprometido ou isolar a rede afetada, a fim de prevenir perdas maiores ou roubo de informações durante ataque;
- Modificar políticas de roteamento de equipamentos de rede ou bloquear padrões de tráfego para interromper o fluxo malicioso;
- Desabilitar serviços vulneráveis para evitar o comprometimento de outros sistemas.

Em seguida, pauta-se a erradicação do incidente, tendo por objetivo eliminar as causas do incidente. Nesse sentido, deve-se procurar:

- Certificar-se de que as causas do incidente foram completamente removidas, incluindo todas as atividades e arquivos associados;

- Garantir a eliminação de todos os métodos de acesso utilizados pelo invasor, como novas contas de acesso, ou, se for o caso, o acesso físico ao sistema comprometido.

Por fim, há a necessidade de restauração do sistema ao seu estado normal. Assim, faz-se necessário:

- Restaurar a integridade do sistema;
- Verificar se o sistema foi recuperado corretamente e se todas as funcionalidades estão ativas;
- Implementar medidas de segurança adicionais para evitar futuros comprometimentos;

AVALIAÇÃO DAS AÇÕES REALIZADAS E LIÇÕES APRENDIDAS

Nesta fase, são avaliadas o tratamento do incidente de segurança com dados pessoais e a eficácia das soluções adotadas, mediante:

(I) Relacionamento e documentação, por ocasião do chamado do incidente, das falhas e dos recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões;

(II) Condução do apanhado de lições aprendidas, com outros atores, se necessário, sob o objetivo de discutir erros e dificuldades encontradas na atenuação do incidente de segurança ocorrido, propondo melhorias na infraestrutura

computacional, sobretudo para os processos de respostas a incidentes; e
(III) Comunicação ao segmento corporativo afetado quanto às decisões tomadas para prevenção de incidentes da mesma natureza, caso se tenha consenso de implementar melhorias na infraestrutura de segurança.

De forma geral, com a análise das lições aprendidas, busca-se discutir os desafios enfrentados durante a resolução do incidente, sugerindo melhorias na infraestrutura e nos processos de respostas a incidentes. Ademais, é importante comunicar à área afetada os procedimentos necessários para prevenir incidentes semelhantes.

Emitir o relatório final do incidente

Cabe ao Controlador de Dados Pessoais do CBMDF elaborar e manter atualizado o RIPD (Relatório de Impacto à Proteção de Dados Pessoais), conforme preconizam os Artigos 5º – Inciso XVIII, 6º, 10 – Incisos e §§ e 38, da Lei Federal nº 13.709, de 14 de agosto de 2018 (LGPD), fazendo nele constar as informações gerais acerca de incidente(s) de segurança com dados pessoais no âmbito da Corporação, sobretudo para fins de cumprimento dos caros princípios de tratamento de dados pessoais constantes ao art. 6º da

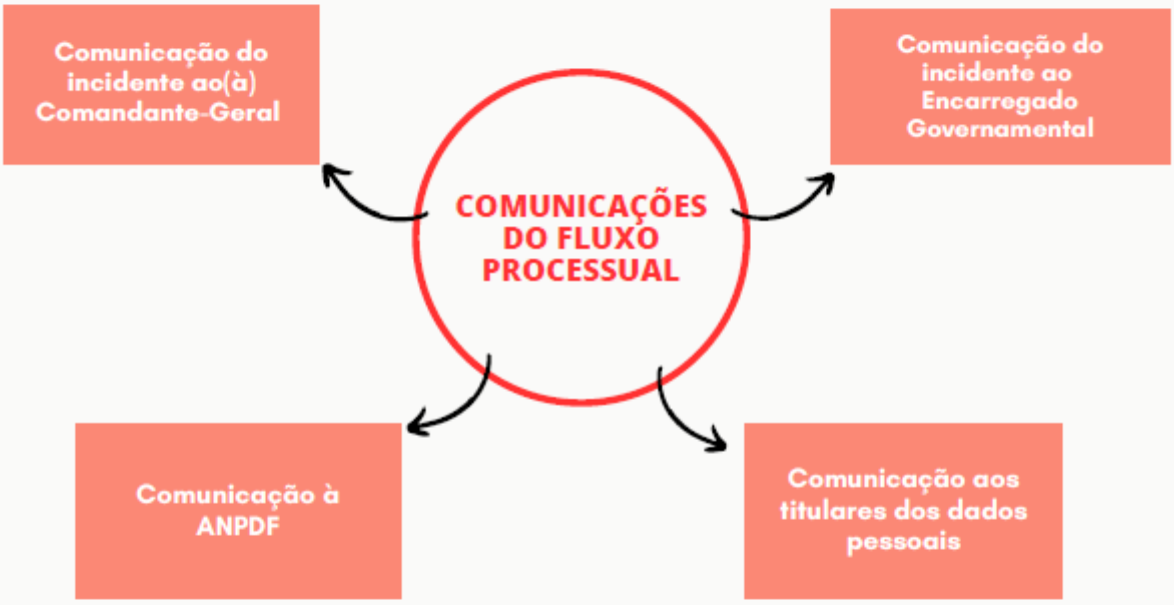
referida Norma, sobretudo o relativo à responsabilização e prestação de contas (Inciso X).

É fundamental documentar todas as informações, evidências e ações envolvidas no tratamento do incidente de segurança de dados pessoais.

FLUXO DE RESPOSTAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

27

FLUXO DE RESPOSTAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS



28

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponivel em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em 12 de setembro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. "Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público". Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico>. Acesso em 12 de setembro de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Formulário de Comunicação de Incidente de Segurança com Dados Pessoais. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>. Acesso em 12 de setembro de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 12 de setembro de 2022.

GOVERNO FEDERAL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf/view>. Acesso em: 12 de setembro de 2023.

GOVERNO FEDERAL Guia de Resposta a Incidentes de Segurança (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf/view>. Acesso em 12 de setembro de 2023.

JUSTIÇA DO TRABALHO. Tribunal Regional do Trabalho da 15ª Região (Campinas-SP). "PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA". Disponível em: <https://trt15.jus.br/legislacao/lei-geral-de-protecao-de-dados-pessoais/manuais>. Acesso em: 12 de setembro de 2023.

FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS - INOVA

1.Registrar Ocorrência

Dados do titular

Posto/Graduação [redacted] Quadro [redacted]

Nome [redacted]

Siape [redacted] CPF [redacted]

Idade 53 Lotação DINAP Condição Titular

Nascimento [redacted] Data e Hora 31/10/2023 - 16:58:41

Celular Whatsapp [redacted]

E-Mail [redacted]

Atualizar Contato

Dados Vazados

Selecione

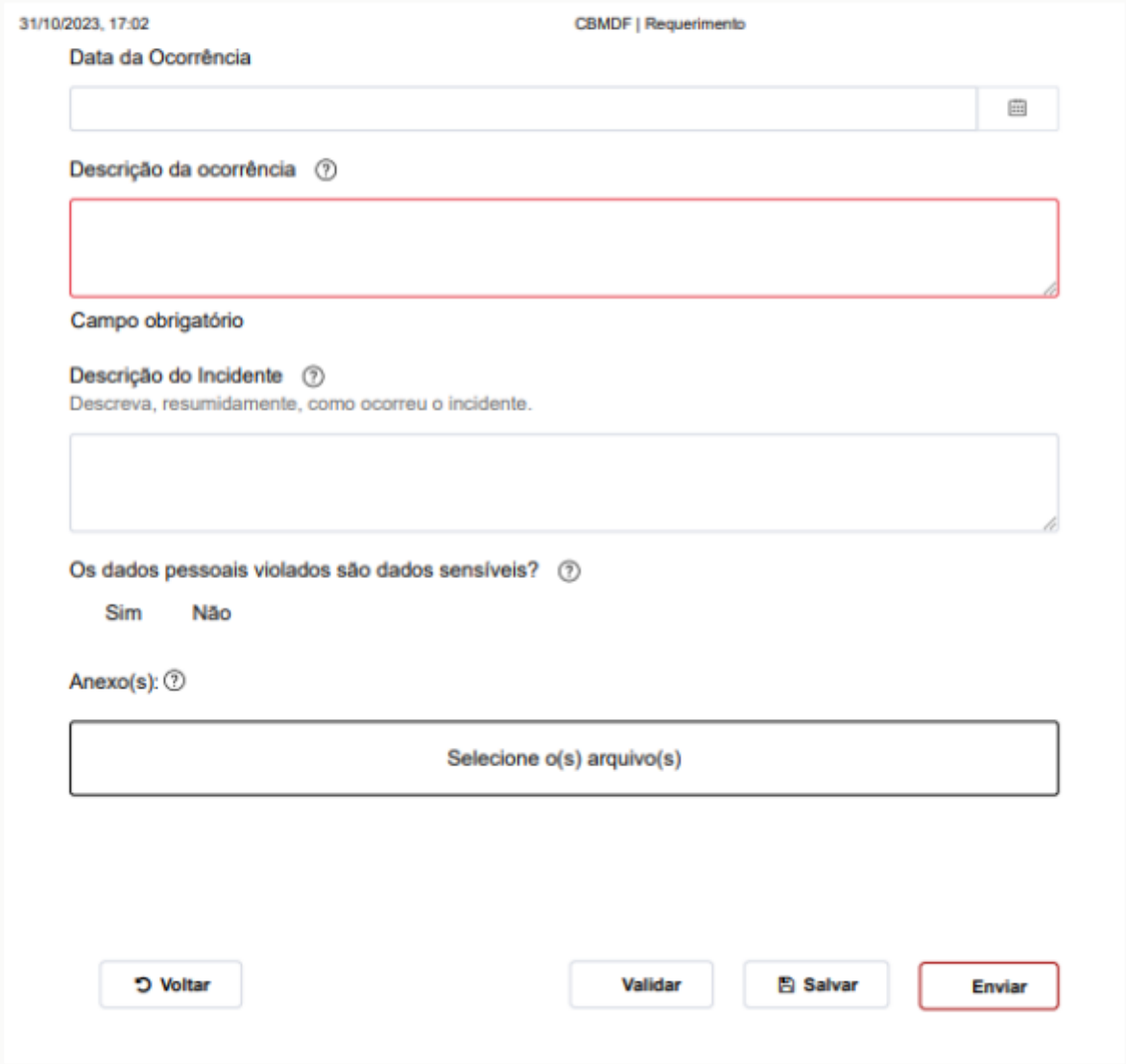
Tipo de incidente

Selecione

://singular.cbm.df.gov.br/inova/externo/rascunhos/editar/13&AL=true 1/2

31

FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS - INOVA



[VOLTAR]