PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA E PRIVACIDADE

Araçoiaba da Serra/SP - 2022

Prefeitura Municipal de Araçoiaba da Serra
15 3281-7000 | www.aracoiaba.sp.gov.br | lgpd@aracoiaba.sp.gov.br
Av. Luane Milanda de Oliveira, 600, Jd. Salete, Araçoiaba da Serra/SP | CEP 18.190-000

Sumário

Preâmbulo

A informação em conjunto com a tecnologia é uma diretriz básica para o funcionamento estratégico e operacional de qualquer governo na esfera municipal.

Desta forma, a Prefeitura Municipal de Araçoiaba da Serra, no advento da implantação da Lei Geral de Proteção de Dados (Lei 13.709/2018), entendendo a necessidade de proteger os Dados Pessoais de seus colaboradores, contribuintes, e outros, obriga-se a manter a transparência sobre o uso dos dados bem como da informação sobre incidentes e medidas tomadas para prevenção e para mitigação dos riscos.

Outrossim, o Plano de Impacto descreve a forma como a Prefeitura Municipal de Araçoiaba da Serra vai responder aos eventos que venha a ferir o direito do titular dos dados, isto é, quais serão as estratégias e planos de controle de danos.

Considera-se incidente de segurança toda violação da segurança que venha provocar, acidentalmente ou intencionalmente, a destruição, alteração, perda, divulgação ou acesso não autorizado a dados pessoais armazenados e mantidos por esta municipalidade para tratamentos com finalidade definida.

O Plano de Resposta a Incidentes deverá ser conhecido integralmente por todos os servidores da Prefeitura Municipal de Araçoiaba da Serra para que num eventual incidente tenham o conhecimento das medidas a serem tomadas.

I – OBJETIVO

O Plano de Resposta a Incidentes de Segurança e Privacidade tem por objetivo nortear as respostas da Prefeitura Municipal de Araçoiaba da Serra em situações de emergência e exceção, sempre documentando formalmente afim de manter a confidencialidade e autenticidade das evidências para que seja possível evitar a repetição dos mesmos incidentes, bem como o atendimento às exigências legais de transparência e comunicação.

Deverá ser aplicado o conteúdo deste documento em qualquer incidente envolvendo Dados Pessoais, observando conjuntamente as demais políticas da Prefeitura Municipal de Araçoiaba da Serra.

Esse Plano tem vigência a partir da sua publicação, por prazo indeterminado, podendo ser revisto e alterado sempre que se identifique a necessidade.

II – DEFINIÇÕES

Agentes de tratamento: Pessoa natural ou jurídica de direito público ou privado que realize tratamento de dado pessoal, podendo ser controlador ou operador;

Anonimização: é a técnica que remove ou modifica informações que possam identificar uma pessoa.

Ataque: evento de exploração de vulnerabilidades. Ocorre quando há uma tentativa de execução de ações maliciosas, como invasão um sistema, acesso não autorizado à informações confidenciais ou a ação proposital de deixar um serviço inacessível;

Autoridade Nacional de Proteção de Dados - ANPD: é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território nacional;

Controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;

Dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;

Dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;

Encarregado ou Data Protection Officer (DPO): é pessoa física designada pelo controlador, responsável por assegurar o cumprimento da legislação local aplicável e atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

COMISSÃO DE LGPD: Comissão Consultiva instituído pela Portaria nº 364/2022, com o objetivo de dar suporte ao Encarregado na implementação da Lei nº 13.709/2018;

Incidente: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da Prefeitura Municipal de Araçoiaba da Serra ou que ela venha a ter acesso;

Operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. O operador será sempre uma pessoa distinta do controlador;

Tratamento: qualquer operação efetuada sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

Vazamento de dados: qualquer quebra de sigilo ou disseminação de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

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

III – RESPONSABILIDADES

O Plano de Resposta a Incidentes de Segurança e Privacidade tem por objetivo nortear as respostas da Prefeitura Municipal de Araçoiaba da Serra em situações de emergência e exceção, sempre documentando formalmente afim de manter a confidencialidade e autenticidade das evidências para que seja possível evitar

IV – ETAPAS DO PROCESSO

Estruturação das Etapas:

Identificação

Identificar um incidente de segurança é essencial para saber qual medida tomar. Deve-se utilizar de medidas de detecção disponíveis, tais como ferramentas de monitoramento, logs, status e relatórios de firewalls, entre outros. Não menos importante, deve haver um trabalho intenso de sensibilização e capacitação de servidores para que tenham capacidade mínima de identificar e informar eventual vazamento de dados.

Preparação

A resposta a um incidente deve ser executada imediatamente. Não há espaço para erros, é essencial que as práticas de emergência sejam executadas e seus tempos sejam medidos, aprimorando assim a metodologia e estimulando a agilidade e exatidão, obviamente minimizando o impacto de indisponibilidade e dos danos.

Contenção

Após a identificação do incidente, há imediata necessidade de contê-lo, ou de isolá-lo para que mais processos ou sistemas não sejam afetados, mitigando os danos no ambiente. Concomitantemente a contenção deverá ocorrer a execução de medidas que permitam a documentação e registro do incidente, evitando a perda de evidências.

Erradicação

Assim que a ameaça esteja contida, deve-se prosseguir com a remoção da mesma, restauração dos processos e sistemas afetados para que no menor tempo possível o estado original seja reestabelecido.

Recuperação

Nesta etapa os sistemas e processos afetados voltaram a funcionar em ambiente de produção, após as devidas validações, garantindo que nenhuma ameaça persista.

Preceitos Assimilados

Atualizar o Plano de Respostas é essencial para facilitação da atuação em futuros incidentes, basicamente é documentado o que o incidente indesejado contribuiu para o aprendizado.

Documentação

É essencial que o incidente seja documentado integralmente, detalhadamente, com todas as ações realizadas nas etapas descritas acima e o que foi possível aprender com esse evento.

Comunicações

Considerando que a ocorrência de um incidente de segurança pode acarretar risco ou danos aos titulares dos dados, deverá ser emitido um comunicado à ANPD e ao titular. No caso de o incidente afetar um grande número de pessoas, o comunicado poderá ser realizado através de publicações que atinjam os interessados.

V – DESCRIÇÃO DO PROCESSO

Detecção

1. Um novo incidente é informado por pessoa interna/externa à Prefeitura Municipal de Araçoiaba da Serra ou por eventual gatilho no monitoramento. A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, telefone, WhatsApp, devendo todas serem registradas pelo Notificador.

Triagem

2. A Notificação é recebida pelo Encarregado de Dados, que deverá fazer a avaliação preliminar ou indicar a necessidade de composição de uma Equipe de Resposta a Incidentes para realizar a avaliação. Caso não seja necessária a formação de uma Equipe de Resposta a Incidentes, o Encarregado assumirá as fases descritas no fluxo do processo.

3. Na avaliação preliminar, devem ser buscadas informações sobre os sistemas e processos que foram supostamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.
4. Dependendo da avaliação preliminar, incidentes que não envolvam sistemas online e que não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares dos setores pertinentes.

Avaliação

5. Nesta fase iniciará uma avaliação detalhada do incidente pelo Encarregado/Equipe, afim de definir a criticidade do incidente.
6. A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

Volume de Dados Pessoais expostos	Alto
	Médio
	Baixo

Alta Gravidade	Alta Gravidade	Alta Gravidade
Média Gravidade	Alta Gravidade	Alta Gravidade
Baixa Gravidade	Média Gravidade	Média Gravidade

Baixa	Média	Alta
Sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos	
Criticidade	Descrição
Alto	Volume de Dados Pessoais afetado superior a 10% da base de dados da Prefeitura Municipal de Araçoiaba da Serra.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Prefeitura Municipal de Araçoiaba da Serra.
Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Prefeitura Municipal de Araçoiaba da Serra.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças ou adolescentes, dados pessoais sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais identificáveis (nome, e-mail, CPF, endereço, etc), combinados, ou não, com informações comportamentais (histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados Dados Pessoais de difícil identificação

7. Deve-se identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. É importante engajar especialistas dos setores afetados para colaborar, no entanto isso deve ser feito a critério do Encarregado/Equipe a qualquer momento que julgar adequado e viável.

Contenção, Erradicação e Recuperação

8. Os responsáveis pelos sistemas e processos impactados devem ser acionados para opinarem sobre os procedimentos de resposta, contenção e erradicação.
9. O objetivo das medidas de contenção e erradicação é a limitação do dano e isolamento dos sistemas e processos afetados, mitigando os danos. Conforme a necessidade e a autorização obtida junto aos setores competentes, poderá ser realizado o desligamento dos sistemas inteiros ou de módulos ou funcionalidades especificas e alocados comunicados de indisponibilidade para manutenção. Necessária muita cautela para não impactar evidências que poderiam ser usadas para identificação de autoria, origem e métodos utilizados para quebrar a segurança.
10. Em se tratando de incidentes não relacionados a recursos de tecnologia da informação, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância investigativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.
11. A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade, disponibilidade e decisão do responsável pelo sistema e processo.

Comunicações

12. Após a notificação de incidente, o mais breve possível, a situação deverá ser encaminhada à Comissão Municipal de Proteção de Dados, que juntamente com o Encarregado e a Divisão de Assuntos Jurídicos avaliará se houve risco ou dano relevante aos titulares dos dados pessoais impactados.
13. Caso se conclua que houve risco ou dano relevante, com assessoria do Departamento de Comunicação, deverão ser realizadas as comunicações obrigatórias por Lei, contendo informações para os titulares dos dados e para imprensa, além dos relatórios formais para a ANPD.

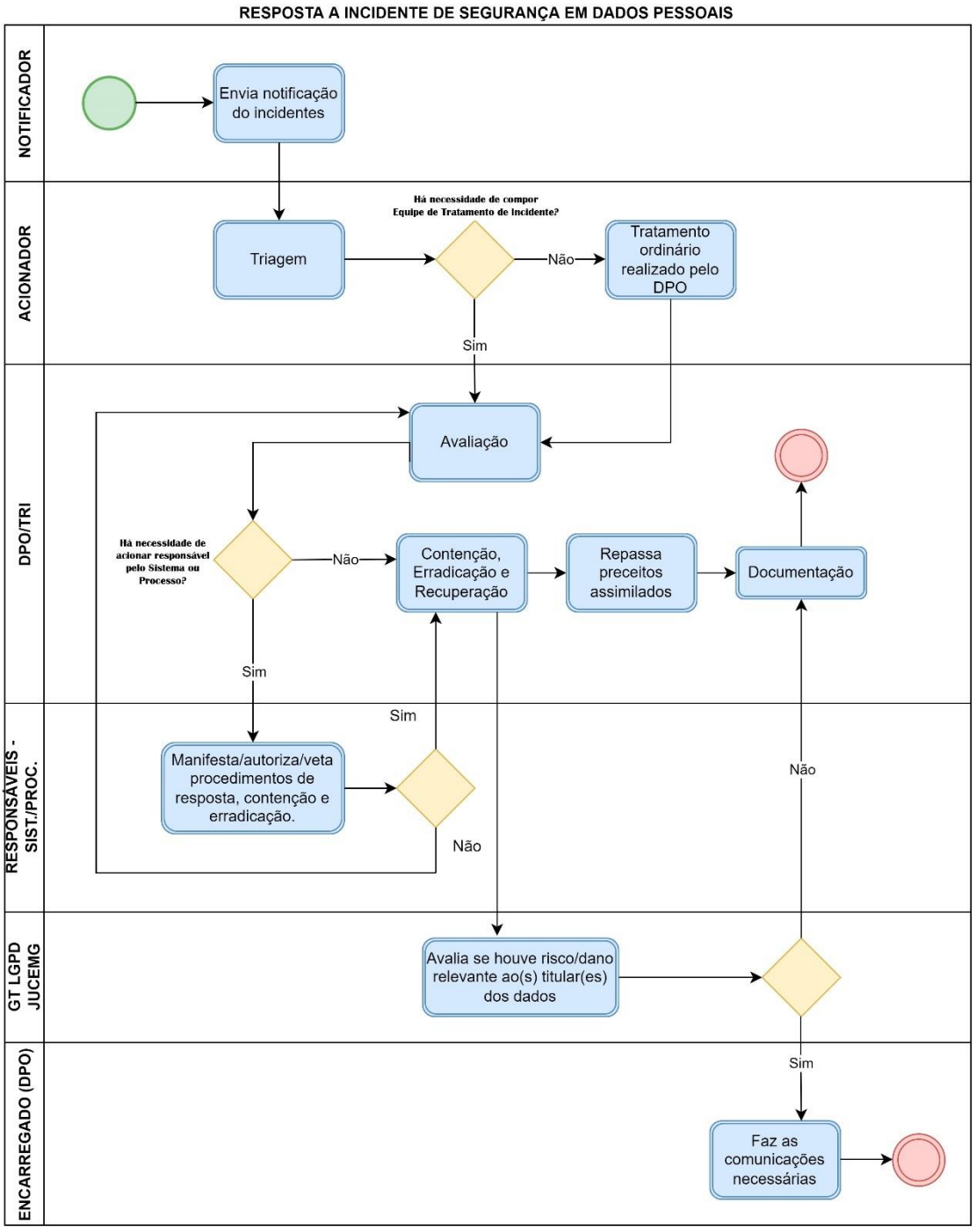
Preceitos Assimilados

14. O encarregado deve documentar o incidente com riqueza de detalhes baseado nas informações obtidas, linha de tempo, quem foram os atores envolvidos, evidencias, conclusões e decisões, bem como as autorizações para ações executadas.
15. Devem ser realizadas Reuniões durante o período de tratativa de crise. Essas reuniões devem gerar relatórios que norteiem a atualização dos procedimentos já existentes ou servir de parâmetro para elaboração de novos procedimentos. Algumas sugestões de perguntas a serem respondidas na Reunião de Preceitos Assimilados:
    a. Onde, quando, como e o que de fato aconteceu?
    b. Qual a eficácia da equipe de resposta a incidentes e de sua gerência neste(s) evento(s)?
    c. Foram seguidos procedimentos já documentados? Em caso afirmativo, eles foram suficientes?
    d. Foi necessário executar procedimentos não documentados? Em caso afirmativo, eles foram executados com sucesso e documentados?
    e. Quais informações anteriores ao incidente foram necessárias?
    f. Foram realizadas quaisquer ações que possam ter prejudicado a recuperação?
    g. O que pode ser atualizado para melhorar o tratamento de incidentes?
    h. Como melhorar o compartilhamento de informações?

i. Quais ações corretivas podem ou devem ser tomadas para evitar incidentes semelhantes no futuro?
j. Quais alarmes e indicadores devem ser observados para detectar incidentes semelhantes no futuro?
k. Quais recursos adicionais podem ser utilizados para detectar incidentes semelhantes?

16. Após a situação estar totalmente controlada, o Encarregado de Proteção de Dados deverá elaborar um relatório circunstanciado com todas as medidas adotadas durante o controle de danos, contendo todas as informações relevantes como dados sobre o incidente, providencias adotadas para preservar evidencias, procedimentos seguidos para conter a crise, medidas técnicas de correção, questionamentos e demandas externas (se houver) e as deliberações da Equipe de Tratamento de Incidentes e da Comissão Municipal de Proteção de Dados.

VI – Fluxo do Processo



VII – CheckList

	Ação	Realizado?
Identificação e Preparação		
1.	Determinar se ocorreu um incidente	
1.1	Analisar os precursores e os indicadores	
1.2	Buscar por informações correlatadas	
1.3	Realizar pesquisa do incidente	
1.4	Documentar, investigar e reunir evidências assim que se identificar a ocorrência do incidente	
2.	Priorizar o tratamento com base em relevância	
3.	Comunicar o incidente às equipes internas envolvidas e, quando necessário, aos atores externos	
Contenção, erradicação e recuperação		
4.	Adquirir, preservar, proteger e documentar 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, repetir as etapas de identificação (1.1, 1.2) para identificar os outros hosts afetados, para então conter (5) e erradicar (6) o incidente em tais hosts	
7.	Recuperar-se do incidente	
7.1	Retornar os sistemas afetados ao estado operacional	
7.2	Confirmar se os sistemas e processos afetados estão funcionando normalmente	
Pós incidente		
8.	Criar o relatório de acompanhamento	
9.	Realizar uma reunião de Preceitos Assimilados (Obrigatória para incidentes graves e opcional para os demais incidentes)	

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentosexternos/anpd_guia_agentes_de_tratamento.pdf >.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >.

Município de Araçoiaba da Serra. **Portaria nº 524 de 3 de agosto de 2022. Normas de Uso dos Recursos de Informática.** Disponível em: < http://aracoiaba.hospedagemdesites.ws/wp-content/uploads/2016/leis/Portaria-524-2022.pdf>.

Paglia, Lucas; Ferola, Bruno; Xavier, Fábio C. **Cartilha de Governança em Proteção de Dados para Municípios**. Salvador, BA; Brasíllia, DF: Editora Mente Aberta; Rede Governança Brasil, 27 de outubro de 2021. [E-book].

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO DAS ALTERAÇÕES	RESPONSÁVEL
01/09/2022	1ª	Plano de Respostas a Incidentes de Segurança e Privacidade - Prefeitura Municipal de Araçoiaba da Serra	**Elaboração:** Kavelyn Vanelly Ferreira **Revisão e Aprovação:** Comissão de Proteção de Dados