PORTARIA Nº 719/2022, DE 27 DE JUNHO DE 2022.

Institui o Plano de Resposta a Incidentes e Gestão de Risco.

O DEFENSOR PÚBLICO GERAL DO ESTADO DA BAHIA, no uso de suas atribuições, conferidas pelo art. 32 da Lei Complementar Estadual nº 26/2006, com as alterações da Lei Complementar Estadual nº 46/2018, RESOLVE publicar o presente Plano de Resposta a Incidentes e Gestão de Risco no âmbito da Comissão para análise dos impactos da Lei Geral de Proteção de Dados - LGPD na Defensoria Pública do Estado da Bahia.

Gabinete do Defensor Público Geral, em 27 de junho de 2022.

RAFSON SARAIVA XIMENES

Defensor Público Geral

PLANO DE RESPOSTA DE INCIDENTES E GESTÃO DE RISCO

Introdução

O Plano de Resposta a Incidentes e Gestão de Risco descreve de forma objetiva como a Comissão para análise dos impactos da Lei Geral de Proteção de Dados - LGPD na Defensoria Pública do Estado da Bahia deve agir perante a um incidente de segurança.

Este plano integra a política de governança em privacidade de dados da Defensoria Pública do Estado da Bahia, segundo o artigo 50, da Lei Geral de Proteção de Dados.

Considerações Gerais

Este documento aplica-se a todo o ambiente físico e tecnológico interno e externo da Defensoria Pública do Estado da Bahia, desde que envolva informações sob a responsabilidade da Instituição.

O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo e descreve a forma como a Defensoria Pública do Estado da Bahia vai responder às situações de rompimento da tríade de Segurança da Informação: **confidencialidade**, **integridade, autenticidade, retratabilidade** e **disponibilidade**.

A resposta da Defensoria Pública do Estado da Bahia deve ser rápida e confiável, ao mesmo tempo resguardando evidências que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

Objetivo

Estabelecer um processo para a gestão de incidentes de Segurança da Informação, possibilitando uma resposta rápida e eficaz a possíveis incidentes, de forma a preservar a reputação e imagem da Defensoria Pública do Estado da Bahia minimizando prejuízos à Instituição, bem como garantindo os direitos e interesses dos assistidos e assistidas.

Esta atividade compreende identificar, prever e descrever situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros.

Aplicação

Aplica-se a toda a base de dados da Defensoria Pública do Estado da Bahia e operadores contratados, isto é, a todos os sistemas, equipamentos, instalações e informações da empresa.

Incidente de Segurança envolvendo dados pessoais

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na 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.

Quando identificado o incidente de segurança que envolva dados pessoais, a Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia seguirá o procedimento estabelecido no item 6 deste Plano.

Resposta a Incidentes de Segurança da Informação e Privacidade

O quadro abaixo descreve o processo que deverá ser seguido pela Defensoria Pública do Estado da Bahia após a identificação de uma falha de segurança:

ID	Agente	Ações a serem adotadas
0	Funcionários, Equipe de TI, Equipe de Infra de TI e Fornecedores ou quaisquer outros que tiverem acesso aos dados sob a guarda da Defensoria Pública do Estado da Bahia	Reportar um incidente de segurança da informação: contato por e-mail (servicedesk@defensoria.ba.def.br) e, se possível, adotar imediatamente as ações necessárias para interromper o vazamento de dados.
1	Encarregados de dados e Equipe de TI; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia (se necessário)	Análise do incidente reportado e coleta de evidências através de canais internos: registros do servidor, evidências, e-mails, capturas de tela, registros da estação de trabalho, equipamentos de rede e servidores. Preservar, na medida do possível, todas as evidências, para que seja possível identificar a causa raiz do problema. As evidências podem ser úteis para demonstrar às autoridades regulatórias que a Instituição teve uma resposta adequada e tratou o incidente com a gravidade necessária. A guarda das evidências digitais devem sempre observar os princípios da (integridade e autoria), deste modo, a depender do caso a Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia ou o Encarregados de Dados poderão orientar sobre a melhor forma de guarda da evidência, seja: (1) por meio de registro de ata notarial; (2) calcular o hash do arquivo; (3) https://www.verifact.com.br; ou outras ferramentas disponíveis e indicadas pelo Encarregados de Dados e pela Comissão.
2	Encarregados de Dados; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia (se necessário)	Análise do incidente envolve: dados de negócios, dados pessoais ou impacto de incidentes no ambiente computacional. A violação de dados pessoais exigirá atenção específica de acordo com os requisitos da LGPD**.**
3	Encarregados de Dados	Classificação do Risco do Incidente: Baixo, Médio ou Alto – conforme critérios e orientações da ANPD.
4	Equipe de TI; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia (se necessário)	Informar imediatamente ao Defensor Público-Geral e aos Encarregados de Dados nos casos que apresente risco (médio ou alto) ao funcionamento da Instituição e aos titulares de dados pessoais.
5	Encarregados de Dados	Mobilizar as áreas da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia que precisam ser envolvidas. Revisar o impacto, estabelecer um plano de ação com responsáveis e prazos. Se o incidente envolver dados pessoais, deve-se observar, além dos planos técnicos,

		outras medidas que precisam ser adotadas previstas na LGPD.
6	Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Para os incidentes de RISCO ALTO, a fim de auxiliar na identificação dos responsáveis pelo incidente, avaliar a possibilidade de acordo com critérios avaliados pelo Encarregados de Dados, de Registrar um Boletim de Ocorrência na Delegacia do local do fato, se possível, buscar uma Delegacia especializada em Crimes Cibernéticos/Digitais.
7	Encarregados de Dados; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Executar os Planos de Ação definidos.
8	Encarregados de Dados; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Conter o incidente, isolando a falha.
9	Encarregados de Dados; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Bloquear e eliminar o problema.
10	Equipe de TI da Defensoria Pública do Estado da Bahia	Se o incidente resultar em perda de Banco de dados (digital), prosseguir com as seguintes medidas para recuperação do banco: - Restauração do arquivo de backup completo digital do banco de dados, considerando o arquivo de backup de log de transação do banco; - Restauração do servidor virtual; - Ativar o Site D.R (Desaster Recovery).
11	Encarregados de Dados; outros integrantes da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Se o incidente resultar em perda de Banco de dados pessoais físicos, a Defensoria Pública do Estado da Bahia deverá utilizar, provisoriamente, os dados disponíveis em sistema próprio, avaliando se será necessário coletar novamente a cópia de documentos e novas assinaturas em documentos originais.
13	Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Transferir lições aprendidas e criar relatórios analíticos com os resultados para possível apresentação periódica à Administração Superior.
14	Encarregados de Dados	Apresentação dos relatórios para a Administração Superior.
15	Encarregados de Dados	Processamento do dia a dia, com atualização do status do incidente em relatório próprio, até a sua finalização.
16	Encarregados de Dados	Fechamento do incidente e registro do fechamento do incidente no relatório próprio.

Se o incidente de segurança envolver dados pessoais, além dos processos técnicos acima, o Encarregados de Dados convocará as áreas da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia que deverão participar das seguintes tarefas:

ID	Agente	Providências	Ação
0	Encarregados de Dados e as áreas da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Avaliar internamente o incidente: natureza, categoria e quantidade de titulares de dados afetados, classificação e quantidade dos dados afetados, consequências concretas e prováveis	Utilizar o FORMULÁRIO (ANEXO 1) como parâmetro, pois são as informações exigidas pela ANPD em caso de incidentes com dados pessoais
1	Encarregados de Dados	Registro do incidente e das evidências dos Planos de Ação executados	Registrar o incidente em relatório próprio para gestão do Programa de Governança de Dados, guardando todas as evidências acerca dos Planos de Ação executados, para fins de prestação de Contas (Art. 6º, X da LGPD)
2	Encarregados de Dados e as áreas da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia	Elaborar e executar Plano de Ação com as medidas de segurança, técnicas e administrativas, que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados	De acordo com os riscos envolvidos, elaborar um plano com prazos e responsáveis, com medidas técnicas ou administrativas, orientações ou benefícios para reverter ou mitigar os riscos dos titulares. (Ex: comunicação com orientações e cuidados que devem ser adotados; troca de senhas; e afins)
3	Encarregados de Dados, Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia e Administração Superior da Defensoria Pública do Estado da Bahia	Avaliar se é necessário comunicar a ANPD e os titulares dos dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD)	Critérios mais objetivos serão objeto de futura regulamentação pela ANPD. De toda forma, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.
4	Encarregados de Dados	Sendo a Defensoria Pública do Estado da Bahia Operadora de uma base de dados, o incidente deverá ser reportado ao Controlador dos dados	Enviar comunicado formal ao Controlador, mediante preenchimento do FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE (ANEXO 1).
5	Encarregados de Dados e Marketing (para comunicação aos Titulares)	Comunicar a ANPD e os titulares dos dados (Parcial ou Completa)	A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, § 1º), conforme será definido pela ANPD.
6	Encarregados de Dados	Acompanhar o andamento do incidente, dos	Comunicar os titulares de dados pessoais, no mesmo

		respectivos impactos e eventuais reclamações dos titulares; reportar a ANPD qualquer novidade; Entregar para a ANPD ou qualquer outra autoridade documentação ou relatório eventualmente solicitado; e acompanhar eventuais reflexos administrativos (multas) e judiciais (processos dos titulares dos dados)	prazo, pelos meios de contato disponíveis, sejam eles: E-mail, telefone, site institucional ou outras mídias digitais oficiais

Disposições Finais
O presente documento detalha o processo de Resposta a Incidentes de Segurança da Informação e Privacidade de Dados a ser seguido pela Equipe da Defensoria Pública do Estado da Bahia.
Durante o plano são propostos Planos de Ações de Comunicação, Restauração e Melhorias, que devem ser definidos entre as equipes envolvidas de acordo com cada caso.
A Defensoria Pública do Estado da Bahia, seus servidores, estagiários, colaboradores e todos aqueles que estejam envolvidos com suas atividades, devem submeter-se não somente ao Plano de Resposta a Incidentes de Segurança da Informação e Privacidade, mas também a qualquer lei, estatuto, regulamento ou contrato aos quais a Instituição esteja sujeita.
Violações a este plano estão sujeitas a sanções disciplinares, observadas a natureza e a gravidade da infração, as quais serão definidas pela Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia.
Este Plano entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Comissão para análise dos impactos da LGPD na Defensoria Pública do Estado da Bahia ou da Administração Superior, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

ANEXO I – Plano de Resposta de Incidentes e Gestão de Risco

Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD).

1 - Comunicação
Tipo de comunicação:
☐Completa.
☐Parcial.

Para comunicação parcial:
☐Preliminar.
☐Complementar.

Critério para a comunicação:
☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
☐Não tenho certeza sobre o nível de risco do incidente de segurança.

2- Agente de tratamento
O notificante é:
☐Controlador.
☐Operador.
Se operador, informar se já houve comunicação ao controlador:

Dados do agente de tratamento:
Número do CPF ou CNPJ:
Nome ou Razão Social:
Natureza da Organização (Pública ou Privada):
Endereço:
Cidade:
Estado:
CEP:
Telefone:
E-mail:

Dados do notificante:
Nome:
E-mail:
Telefone:

Dados do encarregado:
☐Mesmos dados do notificante.
Nome:
E-mail:
Telefone:

3 - Incidente de segurança
Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu.

Quando o incidente ocorreu?
[Data e hora]
☐Não tenho conhecimento. Justifique:
☐Não tenho certeza. Justifique:

Quando a organização teve ciência do incidente de segurança?
[Data e hora]

Descreva como a organização teve ciência do incidente de segurança.

Se a comunicação inicial do incidente não foi comunicada no prazo sugerido de 72 horas após ter tomado ciência do incidente, justifique os motivos.

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

4 - Natureza dos dados

Qual a natureza dos dados afetados?
☐Origem racial ou étnica.
☐Convicção religiosa.
☐Opinião política.
☐Filiação a sindicato.
☐Filiação a organização de caráter religioso, filosófico ou político.
☐Dado referente à saúde.
☐Dado referente à vida sexual.
☐Dado genético ou biométrico.
☐Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).
☐Dado financeiro.
☐Nomes de usuário ou senhas de sistemas de informação.
☐Dado de geolocalização.
Outros:

Qual a quantidade de titulares afetados?

Qual a categoria dos titulares afetados?
☐Servidores/as
☐Terceirizados/as
☐Estagiários/as
☐Assistidos/as
☐Crianças ou adolescentes
Outros:

5 - Medidas de segurança utilizadas para a proteção dos dados.

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?
[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?
Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

6 - Riscos relacionados ao incidente de segurança
Quais as prováveis consequências do incidente de segurança para os titulares afetados?

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

7 - Comunicação aos titulares de dados
Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?
☐Sim
☐Não
☐Não sei
Forneça detalhes.

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?