RESOLUÇÃO CRCBA N.º 662, DE 07 DE NOVEMBRO DE 2022

Institui a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade da Bahia e aprova Matriz de Comunicação.

O **Presidente do CONSELHO REGIONAL DE CONTABILIDADE DA BAHIA**, no exercício de suas atribuições legais e regimentais,

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando que 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;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término;

Considerando o relatório de Auditoria de TI com análise e apresentação dos principais pontos de avaliação, recomendação e Diagnósticos de Maturidade em relação as necessidades elencadas em proposta de projeto elaborado para o CRCBA em relação a avaliação de controles COBIT (em suas versões 4.1 e 5),

R E S O L V E:

Art. 1º Aprovar ad referendum do Plenário, a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade da Bahia e Matriz de Comunicação conforme Anexo.

CAPÍTULO I

DA POLÍTICA E DAS DEFINIÇÕES

Art. 2º Fica instituída a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade da Bahia (CRCBA).

Art. 3º Para os efeitos desta resolução, entende-se por:

I – Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso significa que um dado é considerado pessoal quando permite a identificação direta ou indireta da pessoa natural;

II – Dado pessoal sensível: 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;

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

IV – Tratamento: toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transparência, difusão ou extração;

V – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso desta política, o CRCBA.

VI – Encarregado: 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);

VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – Comitê Gestor de Privacidade e Proteção de Dados (CGPPD): comitê responsável pela avaliação dos mecanismos de tratamento, privacidade e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento com vistas ao cumprimento das disposições da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do CRCBA;

IX – Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional;

X – Notificação: ato ou efeito de informar ou de dar a conhecer sobre uma ocorrência e/ou incidente de segurança com dados pessoais.

CAPÍTULO II

DO OBJETIVO

Art. 4º A Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCBA tem por objetivo descrever os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

Art. 5º É um incidente de segurança com dados pessoais qualquer evento adverso confirmado, 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.

CAPÍTULO III

DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 6º A identificação do incidente pode ocorrer das seguintes formas:

I – denúncia por parte de titular ou terceiro;
II – reporte por parte do operador;
III–pelo emprego de ferramentas automatizadas que detectam vazamentos de dados;

Art. 7º Todas as violações de dados pessoais devem ser comunicadas ao Encarregado pelo tratamento de dados pessoais do CRCBA, sem demora injustificada, para registro e avaliação das medidas a tomar.

Art. 8º Em caso de um incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao Encarregado pelo tratamento de dados pessoais do CRCBA, pelo *e-mail dpo@crc-ba.org.br, no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente.*

Art. 9º No caso do titular ou terceiro, a comunicação de um incidente de segurança com dados pessoais poderá ser enviada ao Encarregado pelo tratamento de dados pessoais do CRCBA, pelo *e-mail dpo@crc-ba.org.br*, preferencialmente, em até *48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.*

Art. 10º Na comunicação, o operador, terceiro ou titular dos dados pessoais deverá descrever sucintamente o incidente ocorrido, atentando para informações, tais como:

I – descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registros de dados pessoais em causa;
II – descrever as consequências prováveis da violação de dados pessoais;
III – descrever as medidas adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Art. 11. O Encarregado pelo tratamento de dados pessoais do CRCBA será responsável pelo registro e análise inicial do incidente e pela resposta sobre o incidente relatado.

Art. 12. Após o registro e a análise inicial do incidente, o Encarregado pelo tratamento de dados pessoais do CRCBA compartilhará a comunicação com o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) do CRCBA, que fará a avaliação das medidas a tomar.

§ 1º Caso necessário, o CGPPD poderá acionar a Comissão de TI (CTI) e a Assessoria Jurídica do CRCBA.

§ 2º O CGPPD não realiza procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

Art. 13. As partes envolvidas devem seguir as orientações do Encarregado pelo tratamento de dados pessoais do CRCBA, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais.

Art. 14. As partes envolvidas devem manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto incidente com dados pessoais e a identificação do autor do incidente.

CAPÍTULO IV

DA NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 15. O CRCBA notificará a ANPD e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

§ 1º O CRCBA deverá avaliar internamente a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular.

§ 2º Para a avaliação interna, deverão ser analisados os incidentes que envolvam especialmente:

I – dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou que tenham 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; e

II – volume de dados envolvidos, 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.

§ 3º A notificação não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

16. Caso necessária, a notificação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV – os riscos relacionados ao incidente;
V – os motivos da demora, no caso de a comunicação não ter sido imediata;
VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 17. Caso não seja possível fornecer todas as informações no momento da notificação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que no momento da notificação preliminar deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

Art. 18. A notificação à ANPD será feita por intermédio do Encarregado pelo tratamento de dados pessoais do CRCBA.

Parágrafo único. O Encarregado pelo tratamento de dados pessoais do CRCBA comunicará o incidente com dados pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pelo CGPPD, pela CTI e pela Assessoria Jurídica do CRCBA.

Art. 19. O Encarregado pelo tratamento de dados pessoais do CRCBA ainda tem como responsabilidade:

I – aprovar e autorizar a divulgação de comunicado aos titulares envolvidos no incidente com dados pessoais;
II – validar quaisquer comunicados ao público, imprensa e usuários;
III – orientar e/ou informar as equipes interessadas a respeito das práticas a serem adotadas com relação ao incidente com dados pessoais;
IV – coordenar todas as ações decorrentes do incidente com dados, com o intuito de mitigar os impactos percebidos;
V – atuar como porta-voz do CRCBA perante a ANPD, demais autoridades competentes e os usuários, supervisionando os contatos e comunicações com o público, decorrentes do incidente com dados pessoais, dentre outras atividades.

Art. 20. Esta Resolução entra em vigor em após a sua publicação.

ANDRE LUIS BARBOSA DOS SANTOS:79734766520
Assinado de forma digital por ANDRE LUIS BARBOSA DOS SANTOS:79734766520
Dados: 2022.11.08 12:46:42 -03'00'

Contador **André Luís Barbosa dos Santos**
Presidente

MATRIZ DE COMUNICAÇÃO

Código: FO-016	Emissão: 01/01/2021	Revisão: 02

O QUE COMUNICAR	QUANDO COMUNICAR	QUEM SERÁ COMUNICADO	CANAL DE COMUNICAÇÃO	RESPONSAVEL PELA COMUNICAÇÃO
Política do SIG	Anualmente ou de acordo com a revisão	Toda Organização	Treinamento, *EAD* e Quadro de Gestão à Vista.	Qualidade
Políticas do SGSI	Anualmente ou de acordo com a revisão	Toda Organização	Treinamento	DIRETORIA
Resultados de Indicadores	De acordo com a periodicidade de cada um	Parte interessada	Quadro de Gestão à Vista/EAD	Qualidade
Resultados das Auditorias	Até 20 dias após a realização da auditoria	Parte interessada	Reunião de Análise Crítica e/ou Divulgação de resultados por e-mail ou EAD	Qualidade
Realização de Auditoria	Até uma semana antes da realização	Toda Organização	Quadro de Gestão à Vista, EAD e *E-mail*.	Qualidade
Resultado de Análise Crítica	Até 15 dias após a realização da reunião de Análise Crítica	Direção e Gestores	E-mail e/ou reunião	Qualidade
Treinamentos Internos	Quando aplicável (antecipadamente)	Parte interessada	Convocação por E-mail	Responsável pelo Treinamento ou designar outro.
Incidente de Segurança da Informação	Imediatamente	Diretoria Geral, Equipe de Segurança da Informação, Fornecedor (quando aplicável)	Verbal e/ou *E-mail conforme Procedimento de Gestão de Incidentes*	Toda Organização
Não Conformidade	Imediatamente	Qualidade	*E-mail ou verbalmente*	Cliente, Toda Organização e Fornecedor
Requisitos Legais	Quando houver atualização	Fornecedor de Software, Qualidade e DIRETORIA	*E-mail ou Reunião*	Diretor Comercial
Autoridade, responsabilidade e	Permanente	Parte interessada	*Treinamentos, reuniões, EAD, Gestão a Vista*	Diretoria Comercial, Qualidade e Coordenador

comunicação de Gerenciamento de Serviço				de Suporte
Reclamação do Cliente	Imediatamente	Departamento de Qualidade e Diretoria Comercial	Telefone, *MySuite* ou *E-mail*	Cliente ou Qualquer que tenha o relato
Admissão ou troca de Função	Quando aplicável e com antecedência	Parte interessada	*E-mail*	Analista da RH
Demissão de Colaborador	Assim que o funcionário for demitido	Parte interessada	*E-mail*	Analista da RH
Efetividade da atualização no Sistema	Quando houver atualização	Parte interessada	E-mail	Fornecedor
Bug's	Quando houver não conformidade no Produto (sistema)	Dono do Produto	E-mail e/ou Telefone e/ou Ticket , Planilha de Bug e Melhoria (considerar Prioridade)	Coordenador de Suporte / Técnico Designado
Melhorias	Proposta de melhoria para o produto	Dono do Produto	Ticket , Planilha de Bug e Melhoria	Coordenador de Suporte/ Técnico Designado
Mudanças que impacte na entrega do serviço ou nos pilares da segurança da informação	Pelo menos uma semana Antes da mudança	Parte Interessada	E-mail, reuniões ou Quadro de Gestão a Vista.	O responsável pelo projeto
Requisito de serviço, requisitos estatutários, regulamentares e as obrigações contratuais	Quando houver alteração	Parte Interessada	Reuniões *ou E-mail*	Diretor Comercial
As mudanças operacionais , táticas e estratégicas que afetam o SIG	Quando houver mudança	Parte Interessada	Reuniões *ou E-mail*	Diretor Comercial e Supervisor de Suporte
Atualização de Documentos	Quando houver atualização	Parte Interessada	*E-mail* e *EAD*	Gestor do departamento ou Qualidade

CRCBA CONSELHO REGIONAL DE CONTABILIDADE DA BAHIA	**MATRIZ DE COMUNICAÇÃO**	
Código: FO-016	Emissão: 01/01/2021	Revisão: 02

Necessidade de Mudança internas e SGSI	Quando necessário	As partes interessadas	Formulário de Mudança - *EAD*	DIRETORIA
Aprovação da solicitação de mudança internas	Quando houver mudanças	Parte Interessada	Formulário de Mudança - *EAD*	O responsável pelo projeto
Implantação no Cliente	Quando aplicável	Cliente e parte interessadas	*Contato telefônico e posteriormente e-mail.*	Suporte Técnico
Contrato	Quando solicitado	Cliente	Atendimento telefônico ou via e-mail	Administrativo
Vendas de Sistemas	Quando solicitado	Cliente	Atendimento telefônico ou via e-mail	Diretor Comercial
Vendas de Equipamento	Quando solicitado	Cliente	Atendimento telefônico ou via e-mail	Administrativo
ANS (Acordo de Nível de Serviço)	Quando solicitado	Cliente	Atendimento telefônico ou via e-mail (link está no contrato)	Diretor Comercial
Demanda/aprovação	Quando houver projeção	Parte interessada	Verbal, via e-mail ou em análise crítica	Diretor Comercial
Campanhas de Compliance e Segurança da Informação	No mínimo Semestralmente ou por demanda	Parte interessada	Verbal, via e-mail ou em análise crítica	Diretoria