RESOLUÇÃO CDN Nº. 371/2021.

POLÍTICA DE GESTÃO DE INCIDENTES COM VIOLAÇÃO DE DADOS PESSOAIS DO SISTEMA SEBRAE

O CONSELHO DELIBERATIVO NACIONAL DO SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS – SEBRAE, no uso da competência conferida pelo art. 14, inciso X, do Estatuto Social do SEBRAE, considerando o EACDN nº 25/2021 enviado pela Diretoria Executiva e em face da deliberação aprovada, por unanimidade, na 4ª Reunião Ordinária, realizada em 29 de abril de 2021,

R E S O L V E:

Art. 1º. Aprovar a Política de Gestão de Incidentes com Violação de Dados Pessoais do Sistema SEBRAE, visando assegurar que incidentes ou possíveis incidentes sejam resolvidos de forma efetiva, com a prioridade adequada, para mitigar o impacto negativo junto aos titulares dos dados pessoais, preservando a imagem do Sistema SEBRAE e seu comprometimento com a proteção de dados pessoais.

Art. 2º. A Política de Governança de Proteção de Dados Pessoais e Privacidade do Sistema SEBRAE, na forma do Anexo Único, é parte integrante desta Resolução, independentemente de transcrição.

Art.3º. Esta Resolução entra em vigor nesta data.

Brasília-DF, 29 de abril de 2021.

JOSÉ ROBERTO TADROS
Presidente do Conselho Deliberativo Nacional

ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 371/2021

POLÍTICA DE GESTÃO DE INCIDENTES COM VIOLAÇÃO DE DADOS PESSOAIS DO SISTEMA SEBRAE

1. OBJETIVO

1.1. O objetivo desta Política é assegurar que incidentes ou possíveis incidentes de violação de dados pessoais sejam resolvidos de forma efetiva, com a prioridade adequada, permitindo o registro, a investigação e a tomada de ação corretiva em tempo hábil para mitigar o impacto negativo junto aos titulares dos dados pessoais, preservando a imagem do **SISTEMA SEBRAE** e seu comprometimento com a proteção de dados pessoais.

2. APLICAÇÃO E ABRANGÊNCIA

2.1. Esta Política é um documento interno, editado com base no Estatuto Social, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos **Dirigentes, Colaboradores, Prestadores de Serviços e Parceiros** do **SISTEMA SEBRAE** ao identificar um possível incidente de violação de dados pessoais, bem como aos envolvidos na resolução do incidente.

2.2. Para os fins desta Política, a referência a:

2.2.1. “dirigentes” abrange Diretores e Conselheiros do SISTEMA SEBRAE;

2.2.2. “colaboradores” abrange empregados, estagiários e aprendizes contratados diretamente pelo **SISTEMA SEBRAE**;

2.2.3. “terceiros” abrange prestadores de serviços e parceiros, empregados de empresas terceirizadas e quaisquer pessoas físicas ou jurídicas que mantenham com o **SISTEMA SEBRAE** qualquer tipo de relação fática ou jurídica;

2.2.4. “usuários” abrange dirigentes, colaboradores e terceiros.

2.3. Esta Política, de abrangência nacional, aplica-se a todo tratamento de dados pessoais realizado pelo **SISTEMA SEBRAE** em território nacional ou com tratamento destinado a indivíduos localizados em território nacional.

2.4. Quando o **SEBRAE/UF** identificar incidentes ou possíveis incidentes de violação de dados pessoais cuja extensão ou gravidade possa afetar a imagem de todo o **SISTEMA SEBRAE**, deve comunicar tal fato imediatamente ao **Encarregado de Proteção de Dados Pessoais do SEBRAE**, a fim de que este avalie a conveniência e oportunidade de avocar a apuração do incidente e de convocar reunião extraordinária do Comitê Estratégico de Proteção de Dados Pessoais do **SEBRAE**, aplicando-se, nesses casos, o disposto nesta Política.

3. PREVENÇÃO A VIOLAÇÕES DE DADOS

3.1. O **SISTEMA SEBRAE** deve realizar avaliações de impacto à privacidade antes de iniciar qualquer projeto ou implementar qualquer tecnologia relacionada ao tratamento de dados pessoais.

3.2. Os incidentes de violação de dados pessoais devem ser prevenidos pelo **SEBRAE** e por cada **SEBRAE/UF** por meio da fiscalização da conformidade, com base nas normas legais e internas, especialmente a Política de Governança de Proteção de Dados Pessoais e de Privacidade do Sistema Sebrae.

3.3. De acordo com o risco identificado, o **SISTEMA SEBRAE** deve tomar as medidas técnicas e administrativas aptas a proteger os dados pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado.

3.4. O **SISTEMA SEBRAE** deve realizar o monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades, registro, monitoramento e análise de trilhas de auditoria e controle de acesso em ambientes físicos e lógicos.

4. IDENTIFICAÇÃO DO INCIDENTE

4.1. Os usuários do **SISTEMA SEBRAE** devem ser capazes de prevenir e detectar um incidente de violação de dados pessoais, bem como estar aptos a promover as medidas de resposta adequadas conforme o caso.

4.2. Todo usuário que identifique um possível incidente de violação de Dados Pessoais deve comunicar imediatamente, por e-mail, o **Encarregado da Proteção de Dados Pessoais do SEBRAE** ou **SEBRAE/UF**, conforme o seu vínculo.

4.2.1. No caso de demora injustificada, o usuário pode responder civil, penal e administrativamente.

4.3. Se o possível incidente ocorrer com dados sob a guarda de um operador que realiza o tratamento de dados pessoais em nome do **SEBRAE** ou **SEBRAE/UF**, o responsável pelo operador deve proceder conforme o disposto em 4.2., sem prejuízo do cumprimento de outras obrigações contratuais específicas.

4.4. O **Encarregado de Proteção de Dados Pessoais do SEBRAE** ou **SEBRAE/UF**, ao receber a comunicação, deve avaliar se os fatos relatados contêm indícios de incidente de violação de dados pessoais.

4.4.1. Caso sejam constatados indícios de incidente de violação de dados pessoais pelo **Encarregado de Proteção de Dados Pessoais do SEBRAE/UF,** cuja extensão ou gravidade possa afetar a imagem de todo o **SISTEMA SEBRAE,** deve comunicar tal fato imediatamente ao **Encarregado de Proteção de Dados Pessoais do SEBRAE.**

4.5. Se os dados objeto do incidente estiverem anonimizados, estes não devem ser considerados dados pessoais.

4.5.1. Nesta hipótese, deverá ser seguido o processo normal de gestão de incidentes de segurança da informação, e não mais tratado o caso em questão como violação de dados pessoais.

5. REGISTRO DO INCIDENTE

5.1. O **Encarregado de Proteção de Dados Pessoais do SEBRAE**, ao receber a comunicação de um possível incidente, ou, de ofício, deve:

5.1.1. avaliar o tipo e o nível de risco da violação de dados;

5.1.2. registrar o incidente na ferramenta de gestão de incidentes do **SEBRAE**;

5.1.3. determinar se o incidente acarreta risco para os direitos dos Titulares dos Dados Pessoais, conforme definição da LGPD;

5.2. O risco deve ser avaliado de forma objetiva, na forma definida no item 7.

5.3. Observado o nível de risco, o **Encarregado de Proteção de Dados Pessoais do SEBRAE**, com o apoio da UASJUR – Unidade de Assessoria Jurídica - do SEBRAE, deve notificar a ocorrência do incidente à ANPD e aos Titulares dos Dados Pessoais.

5.3.1. No caso de vazamentos individuais ou acessos não autorizados, pode haver tentativa de conciliação prévia entre o **SEBRAE** e o Titular e, caso não haja acordo, o **SEBRAE** deverá notificar a ANPD a respeito do incidente e da tentativa frustrada de conciliação.

5.3.2. O **Encarregado de Proteção de Dados Pessoais do SEBRAE** é o responsável, com o apoio da UASJUR e assessorado pela UGM – Unidade de Gestão de Marketing - do SEBRAE, por interagir com o Titular de Dados Pessoais na busca por conciliação prévia direta e com a ANPD.

6. CONTENÇÃO DO INCIDENTE

6.1. O **Encarregado da Proteção de Dados Pessoais do SEBRAE** ou **SEBRAE/UF** deve orientar os gestores e unidades responsáveis ou afetadas pela violação de dados quanto às medidas corretivas a serem tomadas.

6.2. O Gerente da unidade originária do incidente de violação de dados deve tentar, junto com sua equipe, implementar medidas para solucionar o incidente, a fim de mitigar o risco o máximo possível, com o apoio do respectivo **Encarregado da Proteção de Dados Pessoais** e da unidade responsável pela Tecnologia da Informação e Comunicação.

6.3. O **Encarregado da Proteção de Dados Pessoais do SEBRAE** deve estabelecer quem precisa ser informado internamente acerca da violação de dados e quais ações devem ser tomadas por quem foi informado.

6.3.1. Se o **Encarregado da Proteção de Dados Pessoais do SEBRAE** considerar que o incidente pode ter sido causado ou agravado por falhas ou lacunas de normatização ou de procedimento, deve comunicar o Comitê Estratégico de Proteção de Dados Pessoais.

6.4. A unidade responsável pela Tecnologia da Informação e Comunicação deve apoiar com as medidas técnicas necessárias para contenção ou recuperação dos dados relacionados ao incidente, tais como efetuar coleta de evidências ou isolar recursos de tecnologia de modo a não perder informações sobre o incidente.

7. ANÁLISE DE RISCOS

7.1. De forma a analisar os riscos envolvidos no incidente de violação de dados pessoais, o **Encarregado da Proteção de Dados Pessoais do SEBRAE**, com apoio do Gerente da unidade originária do incidente, e quando for o caso, com apoio do **Encarregado da Proteção de Dados Pessoais do SEBRAE/UF,** deve realizar uma análise de riscos considerando pelo menos:

7.1.1. a probabilidade e a gravidade dos riscos;

7.1.2. o tipo de violação;

7.1.3. volume de dados pessoais afetados;

7.1.4. sensibilidade e categoria de dados pessoais afetados;

7.2. Após a análise dos riscos, o **Encarregado da Proteção de Dados Pessoais do SEBRAE** deve fornecer orientações de urgência para o enfrentamento do incidente.

ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 371/2021

8. NOTIFICAÇÃO À ANPD

8.1. Uma violação dos dados pessoais que possa representar riscos altos à proteção de dados pessoais deve ser relatada para a ANPD em até 72 (setenta e duas) horas, contadas a partir do momento em que o **SEBRAE** tomou conhecimento da violação.

8.1.1. Quaisquer possíveis motivos para o descumprimento do prazo previsto em 8.1 devem ser comunicados à ANPD.

8.1.2. Quando não há informações suficientes para comunicar à ANPD com clareza sobre o incidente, um aviso inicial com informações parciais pode ser enviado em até 72 horas após o conhecimento dos fatos. Essas circunstâncias incluem violações complexas que requerem investigações detalhadas ou quando ocorrem várias violações semelhantes em um curto período.

8.2. O **SEBRAE** é considerado ciente de uma violação a partir do momento em que o **Encarregado da Proteção de Dados Pessoais do SEBRAE** verificou a ocorrência de um incidente de dados pessoais ou foi informado por um operador a respeito de um incidente de segurança.

8.3. A notificação à ANPD deve incluir no mínimo:

8.3.1. A descrição da natureza dos dados pessoais afetados;

8.3.2. As informações sobre os titulares envolvidos;

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

8.3.4. Os riscos relacionados ao incidente;

8.3.5. Os motivos da demora, no caso de a comunicação não ter sido imediata;

8.3.6. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;

8.3.7. A identificação de pontos de contato para maiores detalhes;

8.3.8. A descrição das possíveis consequências do incidente de violação de dados;

8.3.9. O elenco das medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

9. NOTIFICAÇÃO AOS TITULARES DE DADOS PESSOAIS

9.1. O **Encarregado da Proteção de Dados Pessoais do SEBRAE**, com auxílio da UASJUR e da UGM do **SEBRAE** deve comunicar violações de alto risco aos Titulares dos Dados Pessoais afetados, em prazo razoável, conforme a ser definido pela ANPD.

9.2. Uma comunicação aos Titulares dos Dados Pessoais deve conter, em linguagem clara e simplificada, a título exemplificativo:

9.2.1. A descrição da natureza dos dados pessoais afetados;

9.2.2. As informações sobre os titulares envolvidos;

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

9.2.4. Os riscos relacionados ao incidente;

9.2.5. Os motivos da demora, no caso de a comunicação não ter sido imediata;

9.2.6. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;

9.2.7. A identificação de pontos de contato para maiores detalhes;

9.2.8. A descrição de possíveis consequências do incidente de violação de dados;

9.2.9. A descrição das medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

9.2.10. A comunicação com os Titulares dos Dados Pessoais deve ser realizada por meios que maximizem as chances de comunicação das informações a todos afetados.

9.3. Se a violação afetar um grande volume de registros de Titulares dos Dados Pessoais, o **SEBRAE** deve decidir se uma notificação pública em massa (transmissão por radiodifusão, por exemplo) pode ser apropriada, em vez de uma notificação personalizada individual, com base em uma avaliação da quantidade de recursos necessários para notificar cada titular de dados individualmente, bem como na avaliação da capacidade de o **SEBRAE** entregar todas as notificações aos titulares dentro do prazo especificado.

10. DECISÃO DE NÃO NOTIFICAÇÃO

10.1. O **SEBRAE** não precisa notificar os titulares de dados pessoais quando o risco do incidente for considerado baixo. Alguns exemplos incluem, mas não se limitam a: (i) violações de dados pessoais publicamente disponíveis; (ii) dados pessoais comprometidos, mas protegidos por uma chave que permanece confidencial e mantida separadamente pelo **SEBRAE** ou **SEBRAE/UF** em ambiente controlado e seguro; (iii)

perdas temporárias de acesso aos dados pessoais; ou (iv) dados pessoais enviados acidentalmente para terceiros confiáveis, em virtude de seu relacionamento com o **SISTEMA SEBRAE**.

10.2. Se for tomada a decisão de não notificar, a justificativa para essa decisão deve ser documentada pelo **Encarregado da Proteção de Dados Pessoais do SEBRAE**.

10.3. O **SEBRAE** deve continuar a monitorar as circunstâncias e os efeitos do incidente, e isso poderá resultar na elaboração ou atualização de notificações à ANPD ou aos Titulares dos Dados Pessoais, conforme o surgimento de novas informações.

10.4. Todas as violações e ações tomadas para responder aos incidentes devem ser documentadas, mesmo que nenhuma notificação seja necessária.

11. PÓS INCIDENTE – PRÓXIMOS PASSOS

11.1. Após a resolução do incidente, a Equipe de Resposta a Incidentes da **Área de Tecnologia da Informação do SEBRAE** deve se reunir para discutir as medidas ou procedimentos de segurança que precisam ser implementados a fim de melhorar a segurança no tratamento de dados pessoais, com base na experiência adquirida durante os procedimentos de resposta.

11.2. A Equipe de Resposta a Incidentes da **Área de Tecnologia da Informação do SEBRAE** deve se manter atualizada com relação a novos procedimentos de resposta às violações, políticas ou protocolos, a fim de aprimorar a qualidade das futuras reações do **SEBRAE** em futuros incidentes.

11.3. A Equipe de Resposta a Incidentes da **Área de Tecnologia da Informação do SEBRAE** deve estar previamente estabelecida e se reunir, de maneira periódica, para a realização de exercícios de simulações para estar preparada a cenários reais que podem surgir no **SISTEMA SEBRAE**.

11.4. A Equipe de Resposta a Incidentes da **Área de Tecnologia da Informação do SEBRAE,** quando perceber aumento das atividades consideradas como possíveis incidentes, deve sugerir que o **Encarregado da Proteção de Dados Pessoais do SEBRAE** realize ações educativas, como palestras e treinamentos corporativos na modalidade “lições aprendidas”, com todos os usuários, para evitar que o referido incidente de segurança ou vazamento volte a ocorrer.

12. DAS RESPONSABILIDADES ESPECÍFICAS

12.1. Encarregado de Proteção de Dados Pessoais do SEBRAE

- Receber a comunicação de incidentes de segurança ou vazamento de Dados Pessoais e dar continuidade ao procedimento;

- Avaliar a necessidade de comunicação do Incidente de Violação de Dados para a Autoridade Nacional de Proteção de Dados e aos Titulares de Dados Pessoais;
- Iniciar processos de investigação do Incidente de Violação de Dados e indicar as áreas envolvidas que deverão participar do processo.
- Determinar as medidas de urgência a serem adotadas para conter ou minimizar os efeitos do incidente.
- Orientar os gestores e unidades responsáveis ou afetadas pela violação de dados quanto às medidas corretivas a serem tomadas
- Notificar o incidente à ANPD e aos Titulares dos Dados Pessoais, quando for o caso, tendo notificado previamente a DIREX.
- Registrar o incidente nos sistemas do SEBRAE.
- Convocar, se for o caso, reunião extraordinária do Comitê Estratégico de Proteção de Dados Pessoais.

12.2. **Encarregado de Proteção de Dados Pessoais do SEBRAE/UF**

- Enviar ao **Encarregado de Proteção de Dados Pessoais do SEBRAE** comunicação de incidentes de segurança ou vazamento de Dados Pessoais.
- Apoiar na implementação de medidas para solucionar o incidente, a fim de mitigar o risco o máximo possível.
- Orientar os gestores e unidades responsáveis ou afetadas pela violação de dados quanto às medidas corretivas a serem tomadas.

12.3. **Área de Tecnologia da Informação**

- Auxiliar na análise dos incidentes de violação de dados pessoais por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;
- Caso o tratamento do incidente envolva impactos no ambiente de produção, a equipe de gerenciamento de mudanças deve ser comunicada para notificar os gestores e usuários do recurso em questão sobre o ocorrido;
- Conduzir em paralelo a este documento os procedimentos indicados na Política de Segurança da Informação e Comunicação;
- Auxiliar nos processos de investigação do incidente quando requerido;
- Apoiar com as medidas técnicas necessárias para contenção ou recuperação do incidente.

- Propor e executar ações ou investimentos que promovam a melhoria contínua do processo de segurança da informação;
- Apoiar sempre que necessário na interação e no escalonamento com as demais áreas a fim de prover um atendimento mais rápido ao processo.

12.4. Equipe de Resposta a Incidentes da **Área de Tecnologia da Informação do SEBRAE**

- Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando eventos que possam causar impacto na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pelo **SISTEMA SEBRAE**.
- Apoiar ao **Encarregado de Proteção de Dados Pessoais do SEBRAE** no cumprimento das fases descritas neste documento desde a Identificação até a solução;
- Comunicar, conjuntamente com **Encarregado de Proteção de Dados Pessoais do SEBRAE,** as áreas responsáveis pelo gerenciamento de mudanças em caso de incidentes de violação de dados pessoais que envolvam impactos no ambiente de produção.
- Auxiliar nos processos de investigação do incidente quando requerido;
- Apoiar com as medidas técnicas necessárias para contenção ou recuperação do incidente.

12.5. **Unidade Jurídica**

- Se o incidente resultar em consequências legais, “deve apresentar o relato dos fatos e a apresentação de indícios relativos ao incidente aos” responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias, se for o caso).

12.6. **Unidade de Comunicação**

- Traçar a estratégia de comunicação com os Titulares de Dados Pessoais e com a ANPD, assim como, se for o caso, com a imprensa ou a comunidade externa.

12.7. **Comissão de Ética**

- Para os incidentes de violação de dados pessoais que envolvam potencial desvio de conduta de colaborador, dirigente ou terceiro em desacordo com o Código de Ética do **SISTEMA SEBRAE**, estes serão encaminhados à Comissão de Ética competente, a qual poderá se aprofundar na investigação.

12.8. **Colaboradores, dirigentes e terceiros**

- Garantir e gerenciar o cumprimento desta Política e demais documentos complementares;
- Reportar incidentes de violação de dados ao **Encarregado da Proteção de Dados Pessoais do SEBRAE** ou **SEBRAE/UF**;
- Estar ciente e manter-se atualizado com esta Política e demais documentos complementares;
- Auxiliar nos processos de investigação do incidente quando requerido.

13. REVISÃO E ATUALIZAÇÃO

13.1. A eventual necessidade de revisão desta Política será avaliada anualmente pelo Comitê de Compliance e Auditoria Externa do CDN, a partir de relatório encaminhado pela Diretoria Executiva do SEBRAE, sem prejuízo de sua alteração a qualquer tempo, caso necessário o seu aprimoramento ou harmonização com outras normas.

14. DOCUMENTOS DE REFERÊNCIA

14.1. Esta Política é complementada pelas Normas e Procedimentos do **SISTEMA SEBRAE**.

14.2. Lei nº 13.709, de 14 de agosto de 2018, Lei de Proteção de Dados Pessoais.

14.3. Decreto nº 8.771, de 11 de maio de 2016, regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

14.4. Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

14.5. Lei nº 12.527, de 18 de novembro de 2011, regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 371/2021

15. DISPOSIÇÕES TRANSITÓRIAS E FINAIS

15.1. O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pelo **SISTEMA SEBRAE**.

15.2. Esta Política, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitados ao **Encarregado da Proteção de Dados Pessoais do SEBRAE**.

15.3. Qualquer dúvida relativa a esta política deve ser encaminhada ao **Encarregado da Proteção de Dados Pessoais do SEBRAE.**

15.4. Os casos omissos deverão ser analisados pelo CDN.

15.5. Esta Política entra em vigor na data de aprovação pelo CDN.