



RESOLUÇÃO CDN Nº. 358/2020.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO 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, incisos X, do Estatuto Social do SEBRAE, considerando o EACDN nº 102/2020 enviado pela Diretoria Executiva e em face da deliberação aprovada, por unanimidade, nas 11ª e 12ª Reuniões Ordinárias, realizadas conjuntamente em 25 de novembro de 2020,

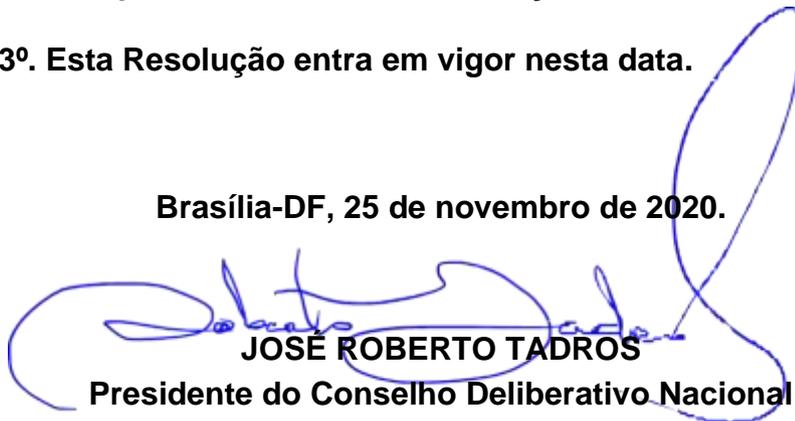
RESOLVE:

Art. 1º. Aprovar a Política de Segurança da Informação e Comunicação do Sistema SEBRAE, visando atender ao disposto na legislação no que tange ao tema de segurança da informação.

Art. 2º. A Política de Segurança da Informação e Comunicação 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, 25 de novembro de 2020.


JOSE ROBERTO TADROS
Presidente do Conselho Deliberativo Nacional



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

Política de Segurança da Informação e Comunicação

SISTEMA SEBRAE



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

ÍNDICE

1. OBJETIVOS	3
2. DECLARAÇÃO DE COMPROMETIMENTO	3
3. APLICAÇÃO	3
4. PRINCÍPIOS.....	3
5. DIRETRIZES GERAIS	4
6. PENALIDADES	7
7. DISPOSIÇÕES FINAIS	7
8. DEFINIÇÕES	8
9. DOCUMENTOS DE REFERÊNCIA	9
ANEXO A - TERMO DE COMPROMISSO E RESPONSABILIDADE PARA DIRIGENTES E COLABORADORES	10
ANEXO B - TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS – PESSOA JURÍDICA	12



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

1. OBJETIVOS

- 1.1. Esta **Política de Segurança da Informação e Comunicação (PSIC)** tem por objetivos:
- 1.1.1. Definir os princípios e diretrizes gerais que visam a preservação da segurança da informação, primando pela confidencialidade, integridade, disponibilidade, autenticidade, bem como legalidade dos processos que amparam a operacionalização e gestão das atividades da Instituição;
- 1.1.2. Estabelecer as responsabilidades e limites de atuação dos **Dirigentes, Colaboradores, Prestadores de Serviços e Parceiros do SISTEMA SEBRAE** em relação à segurança da informação e comunicação, reforçando uma cultura interna baseada em integridade.

2. DECLARAÇÃO DE COMPROMETIMENTO

- 2.1. Os **Dirigentes do SISTEMA SEBRAE** estão comprometidos e apoiam os princípios estabelecidos nesta PSIC de proteção de seus recursos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade com o ambiente legal, primando pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

3. APLICAÇÃO

- 3.1. Esta PSIC é um documento com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, **Dirigentes, Colaboradores, Prestadores de Serviços e Parceiros do SISTEMA SEBRAE**.

4. PRINCÍPIOS

- 4.1. Preservar e proteger as informações sob a responsabilidade do **SISTEMA SEBRAE**, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação (TIC), dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.
- 4.2. Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.
- 4.3. Assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio.
- 4.4. Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da Instituição no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.



ANEXO ÚNICO DA RESOLUÇÃO CDN N°. 358/2020.

5. DIRETRIZES GERAIS

- 5.1. Interpretação:** Esta PSIC e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, no contexto de uso de informações e recursos de TIC, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização do Comitê de Segurança da Informação e Comunicação (CSIC) de cada **SEBRAE**, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.
- 5.2. Publicidade:** Esta PSIC e seus documentos complementares devem ser divulgados aos dirigentes, colaboradores e terceiros, visando a sua disponibilidade para todos os que se relacionam com o **SISTEMA SEBRAE**, ou que, direta ou indiretamente, são impactados.
- 5.3. Propriedade:** As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos dirigentes, colaboradores e terceiros no exercício de suas atividades profissionais com o **SEBRAE**, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de propriedade exclusiva do **SEBRAE** e devem ser empregadas exclusivamente em atividades de interesse institucional.
- 5.3.1.** Quando houver novos **Dirigentes, Colaboradores, Prestadores de Serviços e Parceiros** do **SISTEMA SEBRAE**, deverá ser assinado o **Termo de Compromisso para Dirigentes e Colaboradores** ou **Termo de Compromisso de Segurança da Informação para Terceiros – Pessoa Jurídica**.
- 5.4. Classificação da Informação:** Todas as informações de propriedade ou sob a responsabilidade do **SISTEMA SEBRAE** devem ser classificadas e protegidas com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico, nos termos dos Normativos Internos de Segurança da Informação.
- 5.5. Sigilo:** É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade do **SISTEMA SEBRAE**, por seus dirigentes, colaboradores e terceiros, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja previamente classificada como “pública”.
- 5.6. Privacidade e Proteção de Dados:** O **SISTEMA SEBRAE** respeita a privacidade dos titulares de dados e garante a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte de acordo com a sensibilidade do dado pessoal, a finalidade e a gravidade dos riscos, seguindo a Política de Privacidade e Tratamento de Dados do **SISTEMA SEBRAE**.



ANEXO ÚNICO DA RESOLUÇÃO CDN N°. 358/2020.

- 5.7. Uso dos Recursos de TIC:** Os recursos de TIC de propriedade do **SISTEMA SEBRAE** devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.
- 5.7.1. Os dirigentes, colaboradores e terceiros devem utilizar apenas recursos de TIC previamente homologados e autorizados pelo responsável da TIC de cada **SEBRAE** para a realização de suas atividades profissionais, sejam eles onerosos, gratuitos, livres ou licenciados.
- 5.8. Recursos de TIC Particulares:** O uso de recursos de TIC particulares na execução de qualquer atividade profissional, na interação com os ambientes físicos ou lógicos ou com as informações do **SISTEMA SEBRAE** não poderão ocorrer por meio da rede cabeada e wifi de transmissão de dados, exceto quando autorizado pelo responsável da TIC de cada **SEBRAE**.
- 5.9. Repositórios digitais:** É vedado aos dirigentes, colaboradores e terceiros o uso de repositórios digitais não homologados pelo responsável da TIC de cada **SEBRAE** para armazenar ou publicar informações de propriedade do Sistema Sebrae ou sob sua responsabilidade, salvo casos em que a informação esteja previamente classificada como “pública”.
- 5.10. Mídias Sociais:** A participação do colaborador nas mídias sociais deve ser realizada em acordo com as vedações previstas no artigo sexto do Código de Ética do **SISTEMA SEBRAE** e estar de acordo com norma de Uso de Redes Sociais.
- 5.10.1. Dirigentes, colaboradores e terceiros são responsáveis por suas condutas no uso das mídias sociais. Por isso, cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade, etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.
- 5.11. Controle de acesso:** O **SISTEMA SEBRAE** controla o acesso físico e lógico às suas dependências e aos seus recursos de TIC. Desse modo, dirigentes, colaboradores e terceiros devem possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.
- 5.11.1. Dirigentes, colaboradores e terceiros são responsáveis pelo uso e sigilo de suas credenciais de acesso. Não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.
- 5.12. Áudio, Vídeos e Fotos:** É vedada qualquer atividade relacionada à captura de dados e seu compartilhamento público, inclusive no âmbito acadêmico, na internet e/ou nas mídias sociais, envolvendo gravação de áudio, vídeo ou foto de informações confidenciais, restritas a uso interno, sensíveis ou enquadradas como dados pessoais, que sejam utilizadas na realização das atividades profissionais dentro das dependências do **SISTEMA SEBRAE** por seus dirigentes, colaboradores e terceiros, sem a prévia e formal autorização para tanto, exceto se ocorrer em razão justificável



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

como necessário para cumprimento das atividades profissionais prestadas pelo colaborador.

- 5.13. **Monitoramento:** O **SISTEMA SEBRAE** realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, recursos de TIC e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.
- 5.14. **Inspeção dos Recursos de TIC:** O **SISTEMA SEBRAE**, sempre que considerar necessário, poderá auditar ou inspecionar os recursos de TIC que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os recursos de TIC de propriedade de terceiros, quando autorizada a entrada em suas dependências, independentemente da interação com seus ambientes e informações.
- 5.15. **Documentação:** Cada **SEBRAE** deve estabelecer normas de segurança da informação, relatório de avaliação de riscos e declaração de aplicabilidade para garantir a compreensão e orientar a rápida recuperação em situações de contingência de seus sistemas e processos que envolvam recursos de TIC.
- 5.16. **Conformidade:** O **SEBRAE Nacional** deve possuir e manter um programa de revisão/atualização desta PSIC e de seus documentos complementares. A revisão deve ocorrer a cada dois anos, ou quando mudanças significativas são propostas ou ocorrem, visando a garantia de que todos os requisitos de segurança técnicos e legais implementados sejam cumpridos, atualizados e em conformidade com a legislação vigente.
- 5.17. **Capacitação:** A Universidade Corporativa deve possuir um Plano Contínuo de Capacitação em Segurança da Informação e disseminação a todo o **SISTEMA SEBRAE**, em especial voltado a colaboradores cujas atividades sejam direcionadas a atividades correlatas a segurança da informação e privacidade de dados.
- 5.18. **Conscientização:** O **SISTEMA SEBRAE** deve realizar ações contínuas de conscientização em Segurança da Informação.
- 5.19. **Comitê de Segurança da Informação e Comunicação (CSIC):** Cada **SEBRAE** deve manter um Comitê de Segurança da Informação e Comunicação (CSIC), com composição multidisciplinar, ou seja, formado por representantes de várias unidades internas, cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da Informação e Comunicação, além de avaliar os controles e incidentes relacionados.
- 5.20. **Equipe de Resposta a Incidentes:** Cada **SEBRAE** deve manter uma Equipe de Resposta a Incidentes em Segurança da Informação e Comunicação, interna ou terceirizada, com composição fixa ou variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação.



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

5.21. Canal de Ouvidoria: O SISTEMA SEBRAE possui um canal de Ouvidoria divulgado aos conselheiros, dirigentes, colaboradores e terceirizados para reportar, imediatamente, os possíveis casos de incidentes de segurança da informação e comunicação, podendo fazê-lo formalmente identificado ou com uso de denúncia anônima. Os comunicados categorizados como incidentes de segurança da informação e comunicação serão tratados como prioridade, sendo feito o encaminhamento adequado aos profissionais envolvidos na tratativa dos incidentes.

6. PENALIDADES

- 6.1. Violações:** Os incidentes de segurança da informação identificados como violações devem ser avaliados pelo CSIC correspondente à origem do incidente, que deve elaborar e encaminhar um relatório para a Comissão de Ética do respectivo Sebrae, quando couber, que, após análise, poderá instaurar e apurar as responsabilidades dos envolvidos em procedimento próprio, sugerindo à área gestora da relação a aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, normas e políticas incidentes sobre o regime de pessoal e outros documentos normativos do SEBRAE ou SEBRAE/UF, além da legislação vigente.
- 6.2. Tentativa de Burla:** A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

7. DISPOSIÇÕES FINAIS

- 7.1.** 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.
- 7.2.** Os casos omissos e eventual procedimento diverso do previsto nesta Política de Segurança da Informação e Comunicação serão submetidos à análise do CDN.
- 7.3.** Esta PSIC, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao CSIC de cada SEBRAE.
- 7.4.** Qualquer dúvida relativa a esta PSIC deve ser encaminhada ao CSIC do Sebrae Nacional por meio do e-mail csic@sebrae.com.br.
- 7.5.** As Unidades Federativas do SISTEMA SEBRAE deverão regulamentar em normativos próprios os procedimentos que vierem a ser necessários para operacionalizar as diretrizes aqui estabelecidas, no prazo de até 90 dias a partir da publicação desta Política de Segurança da Informação e Comunicação.
- 7.6.** Esta PSIC entra em vigor na data de aprovação do CDN.



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

8. DEFINIÇÕES

- 8.1. **Autenticidade:** Garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.
- 8.2. **Colaborador:** Empregado, estagiário, menor aprendiz, empregado com contrato de trabalho temporário ou qualquer outro indivíduo ocupante de cargo ou emprego no **SISTEMA SEBRAE**.
- 8.3. **Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.
- 8.4. **Credencial de Acesso:** É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.
- 8.5. **Dirigentes:** Diretores e Conselheiros do **SISTEMA SEBRAE**.
- 8.6. **Disponibilidade:** Garantia de que as informações e os recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.
- 8.7. **Informação:** É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- 8.8. **Integridade:** Garantia de que as informações estejam fidedignas em relação à última alteração durante o seu ciclo de vida.
- 8.9. **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.
- 8.10. **Recurso:** É qualquer coisa que tenha valor material ou imaterial, sendo tangível ou intangível, para o **SISTEMA SEBRAE** e precisa ser adequadamente protegido.
- 8.11. **Recurso Intangível:** Todo elemento que possui valor para o **SISTEMA SEBRAE** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca e conhecimento.
- 8.12. **Recurso Tangível:** caracteriza-se por possuir um corpo físico.
- 8.13. **Repositórios Digitais (Cyberlockers):** Plataformas de armazenamento na Internet, a exemplo, mas não se limitando ao *Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare* e *Scribd*.
- 8.14. **Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

- 8.15. Sigilo profissional:** Trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma organização ou a um grupo, uma vez que a ele é confiada a manipulação da informação.
- 8.16. Tentativa de Burla:** Atos que busquem violar as diretrizes estabelecidas nos documentos normativos do **SISTEMA SEBRAE** e sejam frustrados por erro durante o planejamento ou durante sua execução.
- 8.17. Terceiro:** Prestador de serviço, terceirizado, fornecedor, credenciado, consultor, instrutor e parceiro.
- 8.18. Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do **SISTEMA SEBRAE**.

9. DOCUMENTOS DE REFERÊNCIA

- 9.1.** ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- 9.2.** ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- 9.3.** ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes
- 9.4.** Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.
- 9.5.** Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011.



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

ANEXO A - TERMO DE COMPROMISSO E RESPONSABILIDADE PARA DIRIGENTES E COLABORADORES

Eu [NOME COMPLETO] pelo presente instrumento afirmo cumprir e estar ciente de que:

1. Sou responsável por manter e zelar pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade de toda e qualquer informação de propriedade ou sob a responsabilidade do SEBRAE a mim confiada e/ou por mim acessada em razão de atividades profissionais;
2. Todas as informações disponibilizadas, acessadas e/ou criadas por mim em razão de atividades profissionais são de propriedade e/ou direito de uso exclusivo aos interesses do SEBRAE;
3. Devo agir de forma profissional, cautelosa, ética e legal em relação às informações e recursos de Tecnologia da Informação e Comunicação (Recursos de TIC) de propriedade ou sob a responsabilidade do SEBRAE, além de utilizá-los apenas para fins profissionais, limitados aos interesses do SEBRAE e às atividades contratadas, de acordo com as funções e cargos estabelecidos;
4. Não devo copiar, transferir, compartilhar, alterar, adulterar ou utilizar indevidamente ou para propósitos particulares quaisquer informações de propriedade ou sob a responsabilidade do SEBRAE, além de não praticar quaisquer atos que possam causar prejuízo à Instituição;
5. Devo devolver as informações e recursos de TIC de propriedade ou sob a responsabilidade do SEBRAE imediatamente quando solicitado ou em caso de encerramento das atividades profissionais, além de realizar o descarte seguro das informações do SEBRAE;
6. Estou ciente que o SEBRAE monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados e a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação;
7. Devo comunicar imediatamente, ao meu superior imediato e ao Comitê de Segurança da Informação e Comunicação (CSIC), por meio do e-mail [E-MAIL CSIC UF], qualquer falha, suspeita ou ameaça por mim detectada aos recursos do SEBRAE, como informações, recursos de TIC, ambientes físicos, imagem e reputação;
8. Devo ler, cumprir e manter-me atualizado com a Política de Segurança da Informação e Comunicação (PSIC) do SEBRAE, e demais diretrizes, normas e procedimentos internos da Instituição, publicados e disponíveis para acesso na Intranet;
9. O presente Termo vigorará até o término do contrato ou vínculo relacional com o SEBRAE, contudo as obrigações e responsabilidades em relação ao sigilo, preservação de informações e de direitos de propriedade aqui tratados, permanecem mesmo após o término do contrato ou vínculo relacional estabelecido;
10. Quaisquer atitudes ou ações contrárias ao estabelecido por este Termo, ainda que por mera tentativa de burla, enseja a aplicação das medidas disciplinares ou legais cabíveis;



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

11. Autorizo o SEBRAE a descontar de minha remuneração, diretamente em folha de pagamento, os valores por ele empregados na reparação dos danos causados por minha culpa ou dolo, por mau uso do(s) equipamento(s), uso indevido, inclusive para fins diversos daqueles previstos neste Termo, como por exemplo, para fins particulares (ligações, entre outros), quebra, extravio ou perda do(s) equipamento(s), corrosões decorrentes de exposição do(s) equipamento(s) em condições inadequadas, ou pelo descumprimento de quaisquer obrigações assumidas neste Termo.

Por fim, manifesto nesse ato minha ciência expressa com todas as cláusulas acima, assinando o presente Termo de Compromisso e Responsabilidade.

_____, [DIA] de [MÊS] de [ANO].

[NOME COMPLETO]

N.º da Matrícula:

N.º do CPF:



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

ANEXO B - TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS – PESSOA JURÍDICA

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS – doravante denominado **SEBRAE**, e **[NOME COMPLETO DA PESSOA JURÍDICA]**, já qualificados pelo Contrato [***] celebrado entre as partes em [DIA] de [MÊS] de [ANO], firmam o presente **Termo de Compromisso de Segurança da Informação para Terceiros – Pessoa Jurídica**, passando a ser integrante do referido **Contrato**.

Pelo presente **Instrumento**, as partes têm entre si acordado cláusulas específicas e necessárias para adequada consecução dos serviços contratados, a fim de reger as responsabilidades com relação à **Segurança da Informação** em razão do acesso às **INFORMAÇÕES** de propriedade ou sob a responsabilidade do **SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS - SEBRAE**, aos seus ambientes lógicos e/ou recursos de Tecnologia da Informação e Comunicação.

O/A **[NOME COMPLETO DA PESSOA JURÍDICA]**, pelo presente **Instrumento** afirma cumprir, bem como garantir o cumprimento por seus profissionais, sejam eles funcionários, colaboradores, prepostos, empregados e prestadores de serviços (**Profissionais**), de todas as orientações e determinações especificadas e outras que vierem a ser editadas estando ciente e compreendendo que é responsável por:

1. Prestar os serviços acordados com estrita observância dos preceitos éticos e legais, envidando todos os esforços para atender aos padrões e condições técnicas exigidos, as regras relacionadas ao tratamento de **INFORMAÇÕES** do **SEBRAE** e as melhores práticas de mercado concernentes a Segurança da Informação, tendo como referência as previstas pelas NBR ISO IEC 27001 e NBR ISO IEC 27002;
2. Garantir que os **Profissionais** alocados para execução do presente **Contrato** estejam cientes e cumpram as regras de **Segurança da Informação** estabelecidas por este **Instrumento**, especialmente a **Política de Segurança da Informação e Comunicação (PSIC)** e pelos demais documentos normativos do **SEBRAE**, além daqueles entregues no momento da contratação ou disponíveis para acesso em razão dos serviços contratados;
3. Possuir ou elaborar uma **Política de Segurança da Informação** e acordos de confidencialidade com todos os **Profissionais**, que tiverem acesso ou manusearem as **INFORMAÇÕES** do **SEBRAE** em razão da prestação dos serviços contratados;
4. Assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das **INFORMAÇÕES** do **SEBRAE** no desenvolvimento dos serviços prestados;
5. Utilizarem as **INFORMAÇÕES** e os recursos de TIC do **SEBRAE**, além do acesso aos ambientes físicos e lógicos, **somente para prestação dos serviços contratados**, de acordo com a legislação nacional vigente e a ética;



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

6. Reconhecer que todas as **INFORMAÇÕES** recebidas, criadas ou acessadas por seus **Profissionais** em razão dos serviços contratados são de propriedade exclusiva do **SEBRAE**;
7. Preservar e proteger as **INFORMAÇÕES** a que tiverem acesso, em razão dos serviços contratados, por si e pelos seus **Profissionais**, assim como os recursos de TIC dos diversos tipos de ameaça e em todo o seu ciclo de vida, contida em qualquer suporte ou formato;
8. Utilizar os meios físicos de suporte das cópias das **INFORMAÇÕES** a serem assinalados, quer legíveis humanamente, por equipamentos ou dispositivos (dados eletrônicos), com rótulo de informação “**CONFIDENCIAL**”;
9. Tratar todas as **INFORMAÇÕES** a que tiverem acesso, por si e seus **Profissionais**, como confidenciais, inclusive aquelas que não estejam explicitamente rotuladas;
10. Manter as **INFORMAÇÕES** do **SEBRAE** em segurança e sob sigilo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem autorização, a qualquer terceiro estranho a este **Instrumento** por si e por parte de seus **Profissionais**, ou utilizar de forma contrária ao aqui estabelecido;
11. Não é permitido, por si e pelos seus **Profissionais**:
 - 11.1. Utilizar, reter ou duplicar as **INFORMAÇÕES** que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo **SEBRAE**;
 - 11.2. Copiar, reproduzir, transferir ou usar indevidamente quaisquer **INFORMAÇÕES** para qualquer outra finalidade que não seja a promoção dos serviços contratados;
 - 11.3. Utilizar as **INFORMAÇÕES** de forma que possa configurar concorrência desleal com o **SEBRAE**, tampouco explorá-las em outros negócios ou oportunidades comerciais, assim como promover ou participar no seu desenvolvimento, sem prévia e expressa autorização do **SEBRAE**;
 - 11.4. Modificar ou adulterar as **INFORMAÇÕES** fornecidas pelo **SEBRAE**, bem como subtrair ou adicionar qualquer elemento indevidamente;
 - 11.5. Comentar, compartilhar ou publicar na Internet ou em mídias sociais, ou qualquer plataforma de armazenagem aberta de dados, como repositórios digitais, quaisquer **INFORMAÇÕES** relacionadas à prestação de serviços que tem junto o **SEBRAE**, a não ser que tenha havido prévia e expressa autorização;



ANEXO ÚNICO DA RESOLUÇÃO CDN N°. 358/2020.

11.6. Realizar qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências do **SEBRAE**, exceto quando relacionada a atividade contratada.

12. Respeitar os controles estabelecidos pelo **SEBRAE**, além de garantir o controle automatizado de acessos físicos e lógicos aos ambientes que contiverem **INFORMAÇÕES** do **SEBRAE**, por meio de:

12.1. Controle de acessos a ambientes físicos por dispositivos automatizados com o uso de biometria, senhas, cartão de proximidade ou qualquer outro dispositivo de controle de acesso único;

12.2. Identificação de usuários individuais com o uso de senhas para acesso a sistemas, redes ou qualquer ambiente tecnológico, além de duplo grau de autenticação para acessos críticos;

12.3. Monitoramento, gravação de histórico e auditoria dos acessos relacionados à prestação dos serviços contratados;

12.4. Gravação de acessos de usuários privilegiados.

13. Armazenar as **INFORMAÇÕES** físicas e os dispositivos que as armazenam em ambiente com acesso físico controlado e restrito, por exemplo: gavetas ou armários com chaves;

14. De acordo com a criticidade da informação, armazenar e transmitir as **INFORMAÇÕES** digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia, com chaves de no mínimo 256 bits de criptografia, tais como RSA, RC4, PGP ou compatíveis;

15. Utilizar mecanismo de identificação e autenticação individual, sendo responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros;

16. Utilizar hardware e software licenciados, de acordo com a legislação aplicável, respeitando tratados e convenções internacionais, bem como que estes sejam sempre homologados e autorizados previamente pelo(a) **[NOME COMPLETO DA PESSOA JURÍDICA]**;

17. Respeitar os direitos de propriedade intelectual do **SEBRAE** e de terceiros durante a realização das atividades contratadas;

18. Quando houver uso de dispositivos móveis por parte de **Profissionais**, tais como notebooks, smartphones, tablets, celulares e pendrives, sempre aplicar as medidas de



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

Segurança da Informação relacionadas a cada equipamento, que envolvam desde a implementação e/ou ativação de recursos como uso de senha de bloqueio, bloqueio automático por inatividade, antivírus, antispymware, apagamento remoto até uso de recursos de backup seguro, além de atender os normativos específicos sobre o tema do **SEBRAE**;

19. No caso de haver necessidade de se fazer uso de Repositórios Digitais, a exemplo, mas não se limitando a Google Drive, Dropbox, OneDrive e iCloud, para transmissão de **INFORMAÇÕES** entre as partes, que seja feito o uso de criptografia ou outro método similar que possa garantir a integridade e confidencialidade da informação;

20. Sempre que houver destruição de **INFORMAÇÕES**, inclusive, de cópias, reproduções, reimpressões, traduções ou de materiais que contenham ou relacionem **INFORMAÇÕES**, adotar o “descarte seguro de **INFORMAÇÕES**”, ou seja, papéis e demais **INFORMAÇÕES** impressas deverão ser processadas no picotador de papéis e mídias deverão ser apropriadamente destruídas ou sanitizadas;

21. Devolver ao **SEBRAE**, ou a exclusivo critério deste, descartar todas as **INFORMAÇÕES** que estejam em seu poder, em até 48h (quarenta e oito horas), contados da data da solicitação;

22. Estabelecer procedimentos e processos para treinamento e conscientização das normas e políticas de **Segurança da Informação** para todos os **Profissionais**;

23. Informar imediatamente ao **SEBRAE** todos os incidentes de **Segurança da Informação** que ocorrerem ou puderem ocorrer relacionados à **INFORMAÇÕES** do **SEBRAE**;

24. Reconhecer que o **SEBRAE** realiza o monitoramento de seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à **Segurança da Informação**;

25. Estar ciente que o **SEBRAE** pode auditar ou inspecionar os recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, sempre atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores;

26. Observar e garantir o cumprimento das recomendações acima durante a prestação dos serviços, sendo responsável pelas perdas e danos de qualquer natureza decorrentes de infrações a que houver dado causa pela sua inobservância.

27. Quaisquer atitudes ou ações contrárias ao estabelecido por este Termo, ainda que por mera tentativa de burla, enseja a aplicação das medidas disciplinares ou legais cabíveis.



ANEXO ÚNICO DA RESOLUÇÃO CDN Nº. 358/2020.

Este **Instrumento** obriga as Partes e seus sucessores, a qualquer título.

A omissão ou tolerância do **SEBRAE**, em exigir o estrito cumprimento dos termos e condições deste **Instrumento**, não constituirá novação ou renúncia, nem afetará os seus direitos, que poderão ser exercidos a qualquer tempo.

Este **Instrumento** permanecerá em vigor por prazo indeterminado e, mesmo depois de encerrado o Contrato, o (a) **[NOME COMPLETO DA PESSOA JURÍDICA]** continuará obrigada e responsável com relação às disposições sobre sigilo e preservação dos direitos de propriedade aqui tratados. É vedada a cessão e/ou transferência a terceiros, parcial ou total, dos direitos e obrigações deste **Instrumento**, sem a prévia anuência, escrita, da outra Parte.

As Partes declaram, sob as penas da Lei, que os signatários do presente Instrumento são seus procuradores / representantes legais, devidamente constituídos na forma dos respectivos Estatutos / Contratos Sociais, com poderes para assumir as obrigações ora contraídas.

E por estarem assim, justas e contratadas, as **Partes** celebram o presente **Instrumento**, em 2 (duas) vias, de igual forma e teor, na presença de 2(duas) testemunhas que igualmente o subscrevem.

Brasília/DF, ____ de _____ de _____.

SEBRAE [UF]

C.N.P.J. sob o nº [*]**

[NOME COMPLETO DA PESSOA JURÍDICA]

C.N.P.J sob o nº [*]**

Testemunhas

Nome: [Nome da Testemunha 1]

CPF: [CPF da Testemunha 1]

Nome: [Nome da Testemunha 2]

CPF: [CPF da Testemunha 2]

