1Doc		*Título* **Política de Segurança da Informação**				
Unidade de Negócio	*Área responsável*	*Classificação*	*Aprovação*	*Revisada em*	*Vigência*	*Versão*
Produto e Tecnologia	**Produto e Tecnologia**	**Interna e Externa**	**Diretoria de Tecnologia**	**01/09/2021**	**Indeterminada**	**00**

1. OBJETIVO:

1.1. Estabelecer diretrizes que protejam os dados, pessoais ou não, e os sistemas de informação contra os acessos indevidos e modificações não autorizadas, assim como, garantir a confidencialidade, a integridade e a disponibilidade das informações da 1Doc e de seus clientes.

2. PÚBLICO ALVO:

2.1. Aplica-se a todos os usuários, sistemas ou serviços de propriedade da 1Doc, incluindo todos os indivíduos ou entidades que vierem a ter acesso e/ou utilizar direta ou indiretamente as informações da empresa, incluindo todos os colaboradores, clientes, fornecedores, parceiros e terceiros.

3. RESPONSABILIDADES:

3.1. **É de responsabilidade de todos:**

3.1.1. Cumprir as determinações estabelecidas nessa política, cuja leitura é obrigatória.

3.1.2. Utilizar a informação a que tiver acesso de forma transparente, ética, sigilosa e apenas para a finalidade para a qual a recebeu autorização, sendo proibida qualquer tipo de exposição de dados pessoais de propriedade da empresa 1Doc ou de seus clientes de forma não autorizada, nos termos da legislação.

3.1.3. Estar ciente de sua responsabilidade pessoal no exercício de suas funções quanto ao uso das informações da 1Doc e das informações de seus clientes, tendo o dever de reportar ao departamento de TI da 1Doc qualquer comportamento suspeito, tanto em sistemas internos quanto externos;

3.1.4. Informar ao Comitê de Privacidade previamente sobre mudanças que possam afetar os preceitos de segurança da informação na empresa, nos processos de negócio, nos recursos de processamento e nos sistemas;

3.1.5. Informar ao Comitê de Privacidade sempre que tiver acesso à informação indevida e/ou receber, por engano, informação sobre a qual não deveria ter conhecimento;

3.1.6. Zelar pela segurança e integridade dos recursos disponibilizados para a realização do trabalho e estar ciente de que os mesmos são de propriedade da empresa 1Doc, devendo sua utilização seguir os preceitos estabelecidos;

4. DEFINIÇÕES:

4.1. DIRETRIZES GERAIS:

4.1.1. A empresa 1Doc, ao exercer o papel de fiel depositária de dados, pessoais ou não, e informações de seus clientes, colaboradores, parceiros e fornecedores, proíbe quaisquer práticas que possam gerar benefícios indevidos decorrentes da prerrogativa de sua atuação enquanto organização, especialmente a eventual possibilidade de obter dados e informações não autorizadas devido ao acesso privilegiado às bases de dados, incluindo os dados pessoais;

4.1.2. São proibidas ações deliberadas que visem degradar o desempenho dos recursos de informação ou até mesmo privar um usuário autorizado a acessar os recursos e informações sem a devida justificativa;

4.1.3. As normas descritas no decorrer deste documento devem sofrer alterações sempre que necessário, sendo que estas serão registradas e divulgadas, considerando o tempo hábil para que eventuais providências sejam tomadas;

4.1.4. Quando outras políticas forem mais restritas que esta, a política mais restritiva toma precedência.

4.2. TRATAMENTO DAS INFORMAÇÕES:

4.2.1. As informações e os recursos providos pela empresa 1Doc são de sua única e exclusiva propriedade e/ou responsabilidade, principalmente em razão dos contratos que possua com terceiros, sendo vedado o uso para outros fins que não sejam para atendimento de demandas de seu interesse;

4.2.2. Nenhum colaborador, fornecedor ou parceiro está autorizado a revelar, publicar ou divulgar quaisquer informações de propriedade e/ou responsabilidade da empresa 1Doc sem autorização prévia e formal desta, inclusive informações no âmbito acadêmico e comunidades colaborativas ou repositórios;

4.2.3. A empresa 1Doc é detendora dos direitos patrimoniais relativos às suas marcas, portanto, proíbe o uso não autorizado de suas logomarcas e identidade visual, independentemente de forma ou mídia, incluindo as da internet;

4.2.4. Todos os equipamentos que contenham mídias de armazenamento de dados (ex. pendrive, CD, DVD, folhas para rascunho, CPU, notebook, etc...) devem ser examinados antes da reutilização ou descarte, para assegurar que todos os dados e softwares licenciados tenham sido removidos ou sobregravados com segurança;

4.2.5. Os proprietários de equipamentos cuja propriedade não seja da empresa 1Doc devem garantir a devida proteção contra códigos maliciosos (antivírus atualizado) e o licenciamento correto dos softwares instalados;

4.2.6. Os arquivos relativos a trabalho sempre devem ser salvos em locais com restrição de acesso, tais como Sharepoint, OneDrive, Google Drive, pasta da acesso específico do setor ou atividade, devidamente homologados pela 1Doc;

4.2.7. Os computadores devem sempre estar bloqueados quando o usuário responsável não estiver em frente ao computador, e quando o mesmo trabalhar em documento sensíveis, estes não devem ficar expostos na tela quando houver pessoas não autorizadas diante do mesmo;

4.2.8. Todos os documentos que contenham qualquer tipo de informação sensível (com algum nível de restrição) não podem ficar sobre a mesa ou visíveis.

4.2.9. Informações sensíveis escritas em quadros, paredes ou ferramentas online devem ser apagadas imediatamente após o término da reunião que motivou sua escrita;

4.2.10. Não é permitido comentar sobre assuntos confidenciais de trabalho em locais públicos, incluindo a emissão de comentários e opiniões na internet.

4.2.11. Não é permitido prover recursos ou outras formas de assistência para permitir que pessoas não autorizadas acessem os computadores, pastas ou informações da 1Doc.

4.3. **SENHAS:**

4.3.1. As senhas são de uso individual e sigilosas, não devendo ser compartilhadas, anotadas ou divulgadas a terceiros, incluindo para a equipe de suporte técnico ou de gerenciamento da 1Doc, mesmo quando solicitadas por tais equipes;

4.3.2. A senha deve ser composta de:

- Oito ou mais caracteres;
- Letras maiúsculas e minúsculas
- Ao menos um dígito (0 a 9) ou caractere especial ($, @, *, #, etc...).

4.3.3. Novos colaboradores da 1Doc receberão a primeira senha de acesso por meio de sua gestão e deverão realizar a alteração no primeiro login;

4.3.4. Senhas para contas de administração compartilhadas também são cobertas por esta Política e devem seguir os requisitos aqui definidos.

4.4. **E-MAIL CORPORATIVO DA 1Doc:**

4.4.1. O uso dos serviços de correio eletrônico corporativo deve estar exclusivamente relacionado às atividades e interesses da empresa;

4.4.2. As informações armazenadas ou trafegadas pelo sistema de correio eletrônico corporativo são de exclusiva propriedade da empresa 1Doc;

4.4.3. O titular da conta tem total responsabilidade pelo uso da mesma;

4.4.4. Os recursos de correio eletrônico são limitados por cotas de armazenamento. O titular da conta tem o dever de realizar a manutenção periódica da sua caixa postal, de forma a eliminar conteúdo descartável;

4.4.5. É terminantemente proibido:

- Armazenar e-mails ou qualquer informação da organização na caixa postal particular ou outro meio de armazenamento digital ou impresso;
- Forjar, falsificar ou adulterar quaisquer informações nas mensagens;
- Produzir, transmitir ou divulgar mensagem com informações hostis.

4.5. **TELEFONE:**

4.5.1. Em caso de furto, perda ou roubo de aparelho móvel o colaborador da 1Doc deverá informar imediatamente o setor administrativo/financeiro para o bloqueio da linha.

4.6. **USO DA INTERNET:**

4.6.1. Não é permitido o download e distribuição de conteúdo protegido por direitos autorais ou licença de uso sem o devido licenciamento;

4.6.2. Não é permitido o acesso às páginas cujo conteúdo esteja incluído:

- Conteúdo pornográfico ou relacionados a sexo;
- Atividades ilegais, como: drogas e atos criminosos;
- Atividades que menosprezem, depreciem ou incitem o preconceito a determinado grupo ou classe;
- Conteúdo que promova a violência e terrorismo.

4.7. **INSTALAÇÃO DE SOFTWARES EM EQUIPAMENTOS DA 1Doc:**

4.7.1. A Instalações de software nos equipamentos da 1Doc só podem ser realizados conforme aprovação desta;

4.7.2. É proibida a reprodução ilegal e uso indevido de programas de computador legalmente protegidos, sem a autorização expressa do titular, ou seja, a reprodução é permitida somente com a licença de uso;

4.7.3. Todos os equipamentos de trabalho da empresa devem possuir software para prevenção contra códigos maliciosos (antivírus) instalado e atualizado, sendo proibido ao usuário desabilitar e/ou desinstalar;

4.7.4. Na suspeita da ocorrência de ataque por vírus ou de qualquer outra forma de manifestação de códigos maliciosos, o Comite de Privacidade deverá ser imediatamente notificado;

4.8. **DO TRATAMENTO DE DADOS PESSOAIS**

4.8.1. **Princípios de Proteção de Dados Pessoais**

Os seguintes princípios devem ser observados no tratamento de dados pessoais por todos os envolvidos com a 1Doc, de forma a atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis.

A. Terminologia

Para fins desta Política, as terminologias abaixo serão entendidas como:

LGPD: Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

Dado(s) Pessoal(is): Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dado(s) Pessoal(is) Sensível(is): Todo Dado Pessoal que pode gerar qualquer tipo de discriminação, como por exemplo os dados 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.

Titular(es) de Dados: Pessoa natural singular identificada ou identificável a quem se refere um Dado Pessoal específico.

Tratamento de Dados Pessoais: Qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Controlador: Pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.

Encarregado de Proteção de Dados ou Data Protection Officer ("DPO"): O indivíduo designado como encarregado formal/oficial de proteção de dados,

conforme previsto nas leis de proteção de dados. O DPO pode ser um integrante ou uma pessoa terceirizada.

Consentimento: Manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.

B. Legalidade, Transparência e Não Discriminação:

Os Dados Pessoais devem ser tratados de forma justa, transparente e em conformidade com legislação e regulamentação aplicáveis. Além disso, os Dados Pessoais somente devem ser tratados quando o propósito/finalidade do Tratamento se enquadra em uma das hipóteses legais permitidas, abaixo elencadas, sendo certo que os Titulares de Dados devem ser informados pelo controlador dos dados pessoais sobre a razão e a forma pela qual seus Dados Pessoais estão sendo tratados antes ou durante a coleta:

- necessidade para a execução de um contrato do qual o Titular dos Dados é parte;
- exigência decorrente de lei ou regulamento ao qual a organização está sujeita;
- interesse legítimo pelo Tratamento; e
- necessidade de prover ao Titular dos Dados o exercício regular de direito em processo judicial, administrativo ou arbitral.

Quando o Tratamento de Dados Pessoais não se enquadrarem nas hipóteses acima, e a 1Doc for controlador dos dados pessoais, esta deverá obter o consentimento dos Titulares dos Dados para o Tratamento de seus Dados Pessoais e assegurar que este consentimento e seja obtido de forma específica, livre, inequívoca informada. A 1Doc deve coletar, armazenar e gerenciar todas as respostas de consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser fornecida quando necessário.

Da mesma forma, o Titular de Dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento com a mesma facilidade que foi fornecido.

Em algumas circunstâncias a 1Doc também pode ser obrigada a tratar Dados Pessoais Sensíveis, envolvendo, mas não limitando-se a:

- dados relacionados à saúde ou à vida sexual;
- dados genéticos ou biométricos vinculados a uma pessoa física;
- dados sobre orientação sexual;
- dados sobre condenações ou ofensas criminais;
- dados que evidenciem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas; e

• dados referentes à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O Tratamento de Dados Pessoais Sensíveis é proibido, exceto nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais Dados Pessoais:

• quando for necessário para o cumprimento de obrigação legal ou regulatória;

• quando for necessário para o exercício regular de direitos como, por exemplo, defesa ou proposição de ações judiciais ou administrativas ou arbitrais;

• quando for necessário para o cumprimento de obrigações e o exercício de direitos em matéria de emprego, previdência social e proteção social;

• para proteção à vida ou à incolumidade física do Titular do Dado incluindo dados médicos com fins preventivos, ocupacional;

• para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente,

• quando o Titular dos Dados tiver dado o seu Consentimento explícito, de acordo com a legislação e regulamentação aplicáveis; e

• quando o Tratamento for relativo a condenações penais e infrações ou a medidas de proteção relacionadas será efetuado sob o controle da autoridade pública ou quando o Tratamento for autorizado pela legislação da União ou de um Estado-Membro que preveja as salvaguardas adequadas para os direitos e liberdades dos Titulares de Dados Pessoais.

C. Limitação e Adequação da Finalidade:

O Tratamento de Dados Pessoais deverá ser realizado de maneira compatível com a finalidade original para a qual os Dados Pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro.

D. Princípio da Necessidade (Minimização dos Dados):

A 1Doc somente poderá tratar Dados Pessoais na medida em que seja necessário para atingir um propósito específico. Inclusive, o compartilhamento de Dados Pessoais com outra área ou outra empresa deve considerar este princípio, só podendo ser compartilhados quando os dados pessoais estiverem com um amparo legal adequado.

E. Exatidão (Qualidade dos Dados):

A 1Doc deve adotar medidas razoáveis para assegurar que quaisquer Dados Pessoais em sua posse sejam mantidos precisos, atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao Titular do Dado Pessoal a possibilidade de se requerer a exclusão ou correção de dados imprecisos ou desatualizados.

F. Retenção e Limitação do Armazenamento de Dados:

A 1Doc deve ter conhecimento de suas atividades de Tratamento, períodos de retenção estabelecidos e processos de revisão periódica, não podendo manter os Dados Pessoais por prazo superior ao necessário para atender as finalidades pretendidas

G. Integridade e Confidencialidade (Livre Acesso, Prevenção e Segurança):

A 1Doc deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos Dados Pessoais para protegê-los contra o Tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O Tratamento de Dados Pessoais também deve garantir a devida confidencialidade.

H. Responsabilização e Prestação de Contas:

A 1Doc é responsável e deve demonstrar o cumprimento desta Política, assegurando a implementação de diversas medidas que incluem, mas não se limitam a:

• garantia de que os Titulares dos Dados Pessoais possam exercer os seus direitos;

• registro de Dados Pessoais, incluindo: os registros de atividades de Tratamento de Dados Pessoais, com a descrição dos propósitos/finalidades desse Tratamento, os destinatários do compartilhamento dos Dados Pessoais e os prazos pelos quais a 1Doc deve retê-los; e

• o registro de incidentes de Dados Pessoais e violações de Dados Pessoais;

• garantia de que os Terceiros que sejam Operadores de Dados Pessoais também estejam agindo de acordo com esta Política e com a legislação e regulamentação aplicáveis.

4.8.2. Enquadramento como Controlador/Operador

A 1Doc atuará como operadora dos dados pessoais quando um cliente/parceiro remeter dados pessoais em que seja o controlador ou, ainda, quando um cliente/parceiros remeter contatos pessoais de seus próprios clientes, que poderão ou não serem controlados de tais dados pessoais. Por outro lado, a 1Doc atuará como controlador dos dados pessoais quando definir os tratamentos que deseja realizar, como, por exemplo, dados captados no departamento de marketing, via landing page, hot sites e formulário do website, bem como dos dados pessoais de seus colaboradores.

A 1Doc, quando atuar na figura de operador de dados pessoais, deverá assegurar que o contrato com o controlador dos dados pessoais preveja a implementação de medidas de segurança por ambas as partes, bem como que tal cliente/parceiro, caso atue como controlador, possua a base legal adequada para o tratamento dos dados pessoais e, em qualquer caso, possa a respectiva autorização para a contratação e compartilhamento de dados pessoais com a 1Doc. Por fim, quando a 1Doc atuar na figura de operador dos dados pessoais, esta está somente estará autorizada a tratar Dados Pessoais quando for formalmente solicitado pelo Controlador dos dados pessoais ou quem detenha tal prerrogativa.

4.8.3. **Direitos dos Titulares de Dados Pessoais:**

A 1Doc está comprometida com os direitos dos Titulares de Dados Pessoais, seja quando atuar como controlador de dados pessoais ou quando atuar como operadora dos dados pessoais, os quais incluem:

• a informação, no momento em que os Dados Pessoais são fornecidos, sobre como seus Dados Pessoais serão tratados;

• a informação sobre o Tratamento de seus Dados Pessoais e o acesso aos Dados Pessoais que a 1Doc detenha sobre eles;

• a correção de seus Dados Pessoais se estiverem imprecisos, incorretos ou incompletos;

• a exclusão, bloqueio e/ou anonimização de seus Dados Pessoais em determinadas circunstâncias ("direito de ser esquecido"). Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessário que a 1Doc retenha seus Dados Pessoais para os propósitos para os quais foram coletados;

• a restrição do Tratamento de seus Dados Pessoais em determinadas circunstâncias;

• opor-se ao Tratamento, se o Tratamento for baseado em legítimo interesse

• a retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo para um propósito específico;

• a portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa em determinadas circunstâncias, se aplicável;

• a revisão das decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais; e

• a apresentação de reclamação à 1Doc ou à Autoridade de Proteção de Dados aplicável, se o Titular dos Dados Pessoais tiver motivos para supor que qualquer um de seus direitos de proteção de Dados Pessoais tenha sido violado.

4.8.4. **Prestadores de Serviços Terceirizados (suboperadores):**

A LGPD estabelece que a responsabilidade no caso de danos patrimoniais, morais, individuais ou coletivos derivados de violações à

legislação de proteção de dados pessoais é solidária, i.e., todos os agentes da cadeia envolvendo o tratamento de dados pessoais podem ser responsabilizados pelos eventuais danos causados. Nesse sentido, a possibilidade de a 1Doc ser responsabilizada pelas ações de terceiros implica na necessidade de empregar os melhores esforços para verificar, avaliar e garantir que tais terceiros cumpram com as legislações de proteção de dados aplicáveis.

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções da 1Doc estão sujeitos às obrigações impostas aos Operadores, de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis.

A 1Doc deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Operador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos Dados Pessoais e especifiquem que o Operador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pela 1Doc.

4.8.5. Transferência Internacional de Dados Pessoais

Nas hipóteses em que a 1Doc é autorizada a tratar dados pessoais internacionalmente esta poderá transferir dados pessoais para outros países desde que, alternativamente:

- O país seja classificado como tendo um nível adequado de proteção de dados atribuído pela Autoridade Fiscalizadora ou a transferência seja autorizada por esta;
- Enquanto não houver lista de países de nível adequado divulgada pela ANPD, o país seja classificado pela Comissão Europeia, por meio de uma decisão de Adequação, como país de nível adequado aos critérios da GDPR;
- O agente de tratamento de dados pessoais internacional ofereça à 1Doc pelo menos uma das salvaguardas: a. Códigos de Conduta regularmente emitidos ou binding corporate rules aprovados pela Comissão Europeia; b. Cláusulas Contratuais Padrão emitidas pela ANPD ou pela Comissão Europeia; c. Selos e Certificados de conformidade ou adequação à proteção de dados pessoais concedidos por entidades reconhecidas pela Autoridade Fiscalizadora ou pela Comissão Europeia.
- Obtenha consentimento explícito e destacado dos titulares de dados pessoais para realização de operações de transferência internacional de dados pessoais, com informação prévia sobre o caráter internacional da operação e destacando que o país não tem nível adequado

de proteção de dados reconhecido ou que não há salvaguardas da conformidade do agente de tratamento, conforme o caso. Caso o país não tenha nível adequado de proteção de dados reconhecido ou não haja salvaguardas da conformidade do agente de tratamento, tais informações deveriam ser prestadas ao titular de dados pessoais previamente, a fim de que consinta com os riscos da operação.

A 1Doc se compromete em informar os titulares de dados pessoais, quando for controladora dos dados pessoais e, conforme o caso, aos seus clientes, quando for operadora dos dados pessoais, sobre a ocorrência de operações de transferência internacional de dados pessoais, designando o conjunto de dados encaminhados, a finalidade do envio e o seu destino.

4.8.6. Registro de Ocorrências com relação aos dados pessoais

Todos os destinatários desta Política têm o dever de contatar o Cômite de Privacidade da 1Doc, quando da suspeita ou da ocorrência efetiva das seguintes ações:

- Operação de tratamento de dados pessoais realizada sem base legal que a justifique;
- Tratamento de dados pessoais sem a autorização por parte da 1Doc ou do controlador dos dados pessoais, no escopo das atividades que desenvolve;
- Tratamento de dados pessoais que seja realizada em desconformidade com a Política de Segurança da Informação da 1Doc;
- Eliminação ou destruição não autorizada de dados pessoais de plataformas digitais ou acervos físicos em todas as instalações da Instituição ou por ela utilizadas.

Desta forma, a 1Doc tem um processo interno centralizado para registros de reclamações sobre o tratamento dos dados pessoais. No caso de uma reclamação, quem identificar a realização de um Tratamento ilegal ou inapropriado de seus Dados Pessoais que seja incompatível com a Política de Proteção de Dados, a pessoa que identificar o incidente de violação de dados devera peticionar para o Comitê de Privacidade da 1Doc.

Todos os incidentes e potenciais violações de dados devem ser reportadas, tendo cada colaborador a responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de Dados Pessoais assim que as identificarem. Quando um incidente ou violação real for descoberto é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

4.8.7. **Programa de Conformidade às Leis de Proteção de Dados Pessoais**

O Programa de Conformidade da LGPD da 1Doc visará a garantir o compromisso da 1Doc em zelar pelo tratamento adequado de dados pessoais para fins legítimos que possam ser objeto de suas atividades e reforça o seu compromisso com boas práticas de privacidade e proteção de dados com as seguintes ações:

- Produção e disseminação de informações, independente do formato, que descrevam as responsabilidades individuais dos destinatários desta Política no âmbito da privacidade e proteção de dados pessoais;
- Fornecimento de treinamentos, orientações e aconselhamentos para os empregados da 1Doc e terceiros, incluindo, mas não se limitando a cursos online, workshops, reuniões internas, conversas regulares, palestras, dentre outras iniciativas; comungando conteúdos disponibilizados no formato digital e presencial;
- Incorporação de preocupações e cuidados no tratamento de dados pessoais em todas as etapas de suas atividades, incluindo, mas não se limitando a rotinas administrativas, atividades de pesquisa, prestação de serviços, atividades de cunho acadêmico, dentre outras;
- Identificação e aprofundamento da avaliação dos riscos que podem comprometer o alcance dos objetivos da 1Doc na área de privacidade e proteção de dados pessoais; definir, criar e implementar planos de ação e políticas para mitigar os riscos identificados; além de manter uma avaliação contínua dos cenários com vistas a avaliar se as medidas implementadas não requerem novas diretrizes e atitudes.

A partir da entrada em vigor da LGPD, haverá a nomeação do Encarregado da 1Doc - também referido como Data Protection Officer (1Doc DPO) –, de forma devidamente identificada em seu website, o qual auxiliado pela sua equipe técnica, terá as seguintes responsabilidades:

- Conduzir o Programa de Conformidade da LGPD na 1Doc, zelando pela sua fiscalização;
- Monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas da 1Doc;
- Orientar os destinatários desta Política quanto ao regime de privacidade e proteção de dados pessoais da 1Doc;
- Assegurar que as regras e orientações relativas à proteção de dados sejam informadas e incorporadas nas rotinas e práticas da 1Doc;
- Organizar treinamentos sobre proteção de dados pessoais na 1Doc;
- Prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes (e.g. Ministério Público, Autoridade Nacional de Proteção de Dados Pessoais, etc.);

- Responder às solicitações e reclamações de titulares de dados pessoais cujos dados tenham sido objeto de tratamento por uma unidade da 1Doc.
- Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;
- Elaborar os relatórios de impacto à privacidade e proteção de dados necessários, pareceres técnicos e revisão de documentos no que se refere à proteção de dados.

4.8.8. **Guarda legal e Descarte de dados pessoais**

A 1Doc utilizará os dados pessoais nos prazos necessários para o cumprimento de suas obrigações legais e contratuais, inclusive conforme necessário para a execução dos contratos com Clientes, Fornecedores, Parceiros, Colaboradores e titulares que estejam vinculados a determinadas Políticas de Privacidade de dados pessoais. Além disto, a 1Doc poderá ARMAZENAR tais dados pessoais por prazos superiores às execuções de tais relações, visto que, em diversos casos, terá legislações que a obriguem ou lhe concedam o direito de somente realizar tal guarda legal, inclusive para defesa em eventuais processos judiciais ou administrativos.

5. DATA CENTER E DETERMINAÇÕES DE SEGURANÇA TECNOLÓGICA

A 1Doc possui as seguintes definições de segurança da informação:

5.1. Bancos dados
- 100% hospedados no Brasil
- Acessados somente em rede interna, sem acesso externo
- Descentralizado para garantia de disponibilidade
- Backups periódicos
- Acesso restrito apenas para colaboradores estratégicos e com restrição de escopo
- Embaralhamento de dados sensíveis para acesso de suporte via sistema

5.2. Segurança de Rede / Aplicação
- Testes de intrusão periódicos
- Todo ecosistema de softwares rodam em rede fechada
- Inteligência de Rate Limit para proteção DDOS
- Conformidade com National Institute of Standards and Technology (NIST), sob identificação SP-800-115
- 3 camadas de firewall

5.3. Coberturas contra principais tipos de ataques:
- Injeção de Códigos ou Comandos Arbitrários
- Corrupção de Memória
- Falha em Controle de Acesso e ou Autenticação
- Exposição de Recurso ou Objeto Restrito
- Ausência ou Falha de Criptografia

- Falha em Validação de Upload
- Inclusão Maliciosa de Arquivos
- Falha em Validação de Parâmetros
- Evasão de Controle
- Falha em Política de Senhas
- Exposição de Informação Sensível
- Uso de Configuração ou Mecanismo Depreciado
- Falha em Restrição de Ações Excessivas
- Escalação de Privilégios
- Uso de Componente Vulnerável
- Falha em Validação de Origem
- Indisponibilidade do Serviço
- Deserialização Insegura
- Mensagens de Erro Informativas
- Falha Lógica em Funcionalidade

Todos os serviços em nuvem em conformidade com as políticas de segurança da AWS - https://aws.amazon.com/pt/compliance/programs/ - e com padrões de segurança/certificações PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 e NIST 800-171.

6. SANÇÕES:

6.1. Qualquer violação a esta Política ou à legislação vigente acarretará em sanção aos responsáveis pela ilicitude, podendo os mesmos receber advertência, suspensão ou desligamento da empresa, ou em casos de terceiros, rescisão contratual. Todas as hipóteses sem prejuízo de eventual adoção de providências nas esferas trabalhista, cível e criminal.

7. RELATO DE PREOCUPAÇÕES OU VIOLAÇÕES:

7.1. Se você suspeitar ou tiver preocupações relacionadas à violação da presente Política ou da legislação brasileira, você deve comunicar o Comitê de Privacidade, pelos canais oficiais (privacidade@1doc.com.br).

8. CONTROLE DE REVISÕES:

Revisão	Data	Quem criou/alterou	Revisor	Aprovador	O que mudou
00	01/09/2021	Produto	Tecnologia e Backoffice	Diretoria	Versão Original