Parecer de Segurança da Informação sobre:
Utilização de formulários e edição colaborativa de documentos online ofertados por serviços na nuvem para demandas do TJPE

Este parecer tem como objetivo subsidiar as instâncias decisórias do TJPE com informações pertinentes para deliberação acerca de eventuais iniciativas de utilização de formulários e edição colaborativa de documentos online ofertados por serviços na nuvem para demandas do TJPE. Este parecer está dividido em quatro avaliações: Legal, Normativa, de Termos de Uso e Técnica.

Contexto

Algumas empresas ofertam serviços online para disponibilização de formulários e edição colaborativa de documentos, acessíveis mediante concordância com seus termos de uso. Estes serviços podem permitir que usuários compartilhem documentos, editem documentos de forma colaborativa, criem formulários para preenchimento por outros usuários, compartilhem formulários por meio de links, dentre outras funcionalidades. Todos esses recursos são acessíveis através de um navegador web (algumas funcionalidades podem exigir o uso de plug-ins ou add-ons) e os dados processados são armazenados nos datacenters da empresa que oferta o serviço. Comumente estas empresas oferecem os serviços para uso pessoal sem custo financeiro, embora os termos de uso cedam direitos sobre os dados às empresas provedoras. Para uso corporativo as mesmas empresas oferecem opções de uso do serviço com custos financeiros, em muitos casos expressivos, normalmente cobrado por usuário. São exemplos de serviços com estas características: Google Docs, Microsoft Office Online, Dropbox Paper e Zoho Office. Este parecer se limita ao exame da adoção deste tipo de serviço, apenas nas suas versões para uso pessoal, para demandas do TJPE.

Avaliação Legal

É importante observar a Lei nº 13.709 de agosto de 2018 (Lei Geral de Proteção de Dados), que em seu Art 5º classifica os tipos de dados sobre os quais o TJPE precisa dar tratamento específico para fins de proteção à privacidade:

> ***Art. 5º*** *Para os fins desta Lei, considera-se:*
>
> *I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*
>
> *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 - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;*

O processamento de dados pessoais por parte do TJPE deve sempre ser pautado pelos dispositivos desta Lei. Isto implica na implantação e manutenção de uma série de controles para garantir a devida utilização dos dados, buscando preservar a privacidade do usuário. As formas de atendimento à LGPD pelos órgãos do Poder Público implicam também, no que que couber, no atendimento à Lei nº 12.527 de 2011 (Lei de Acesso à Informação - LAI), Lei nº 9.507 de 1997 (Lei do Habeas Data) e Lei nº 9.784 de 1999 (Lei Geral do Processo Administrativo), como disposto no CAPÍTULO IV - Do Tratamento de Dados Pessoais Pelo Poder Público da LGPD.

Serviços na nuvem de formulários e edição colaborativa disponibilizados para uso pessoal baseiam-se em Termos de Uso que conflitam em vários pontos com a LGPD, pois entregam os dados para o prestador de serviço na nuvem que não possui nenhuma relação contratual com o TJPE. O vínculo é apenas com uma conta

pessoal de um funcionário ou pessoa responsável. Desta forma são difíceis as condições para o TJPE exigir da empresa que atenda aos critérios da LGPD e dificultará qualquer tipo de responsabilização da mesma em caso de incidente. Ademais os Termos de Uso aceitos pelo detentor da conta de acesso ao serviço já cedem direitos sobre os dados e eximem a empresa de responsabilidades.

No que diz respeito a aplicação de serviços de uso pessoal em nuvem como suporte para atos processuais é importante levar em consideração o que dispõe a Lei 11.419 de 2006 (Lei do Processo Eletrônico). É possível destacar como exemplo o Art. 8º e seu parágrafo único:

> **Art. 8º** Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas.
>
> **Parágrafo único**. Todos os atos processuais do processo eletrônico serão assinados eletronicamente na forma estabelecida nesta Lei.

Avaliação Normativa

É mandatório levar em consideração as normas internas do TJPE, que dispõem sobre a classificação da informação, controle de acesso e outros assuntos pertinentes ao objetivo deste parecer.

Resolução nº349/2013 (Política de Segurança do TJPE)

A utilização de serviços na nuvem de uso pessoal conflita com alguns dispositivos da Resolução nº349 de 2013. Estes serviços na nuvem não foram criados para ambientes corporativos, portanto, não dispõem de mecanismos administrativos de controle de acesso. Cada usuário gerencia da forma descentralizada o controle de acesso aos documentos e dados que utiliza. Portanto, torna bastante difícil implementar e manter um controle de acesso como disposto nos Art. 15, Art. 16 e Art. 19:

> ***Art. 15****. Cabe aos responsáveis pela informação a classificação e a definição de quem possui acesso e o tipo de privilégios de acesso, sem prejuízo do disposto na legislação vigente.*
>
> ***Art. 16****. Os agentes judiciários têm o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de interposição de Processo Administrativo, que poderá restar em sanção severa, conforme a gravidade do ato e os prejuízos sofridos.*
>
> ***Art. 19****. O acesso aos ambientes físicos e recursos lógicos de TIC devem ser controlados e restritos às pessoas autorizadas pela SETIC, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível*

Uma das preocupações na adoção de sistemas pelo SETIC é garantir um nível mínimo de auditabilidade e monitoramento dos serviços, como disposto no Art. 25 e seu §1º. No caso da adoção de serviços mantidos por terceiros sem qualquer vínculo contratual este tipo de atuação da SETIC torna-se inviável na prática. Registro e coleta de eventos, análises forenses e auditoria estarão bastante limitados, não sendo possível averiguar satisfatoriamente contestações de usuários, solicitações da Corregedoria Geral de Justiça ou apuração de irregularidades.

> ***Art. 25****. O TJPE, por meio da SETIC, monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo, o e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento.*

> ***§1º** O TJPE também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação, podendo investigar fatos que comprometam seus ativos.*

As preocupações citadas no Art. 25 para a contratação de serviços, inclusive nos moldes do tipo de serviço avaliado neste parecer, de acordo com os Art. 36, Art. 39, Art. 41 e parágrafo único, exigem cuidados com de segurança no uso de sistemas e a assinatura de Termo de Confidencialidade por parte do contratado. No caso dos serviços prestados para fins pessoais não há essa possibilidade, pois a empresa que oferta o serviço não está firmando contrato com TJPE, portanto, não lhe deve garantias e nem a obrigação de assinatura de Termos.

> ***Art. 36**. Todos os relacionamentos e contratações em que haja o compartilhamento de informações ou ativos de TIC do TJPE ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos devem ser precedidos por Termos de Confidencialidade e cláusulas contratuais que tratem especificamente da Segurança da Informação.*
>
> ***Art. 39**. Os Sistemas de Informação adquiridos, mantidos ou desenvolvidos pelo TJPE deverão atender aos princípios e requisitos de Segurança da Informação, estabelecidos pela presente Resolução e demais normas em vigor.*
>
> ***Art. 41**. Os dados classificados como sigilosos, mantidos pelos Sistemas de Informação, não deverão estar replicados ou acessíveis em outro ambiente, sem a competente autorização do NSI, vinculado à SETIC, sob o risco de vazamento de informações pessoais ou confidenciais sob a guarda do TJPE.*
>
> *Parágrafo único. O descumprimento desta disposição acarretará em Procedimento Administrativo disciplinar e justificará a aplicação de penas previstas em lei, conforme a gravidade do ato e prejuízos sofridos pelo TJPE.*

Termos de Uso

Abaixo uma tabela com os links para os termos de uso e privacidade de serviços de ampla utilização nos dias atuais para criação de formulários e edição colaborativa de documentos. Estes links foram utilizados na elaboração deste parecer:

Serviço	Endereço	Data de acesso
Google	• https://policies.google.com/?hl=pt	05/12/2018
Microsoft	• https://privacy.microsoft.com/pt-br/privacystatement • https://www.microsoft.com/pt-br/servicesagreement/	05/12/2018
Dropbox	• https://www.dropbox.com/help/security?utm_source=community&utm_medium=navbar?utm_source=community&utm_medium=navbar	

Avaliação Técnica

Tecnicamente o acesso aos serviços avaliados é quase sempre integralmente por meio de navegador web, portanto, não implicando em grandes dificuldades técnicas. Entretanto, **não há como a SETIC dar garantias sobre a integridade, confidencialidade e disponibilidade dos dados e do serviço**. Alguns pontos merecem destaque:

- Em casos de incidentes não existe um canal entre a SETIC e a empresa provedora para resolução de problemas, pois trata-se de um vínculo entre uma pessoa e a empresa, que não oferece garantias amplas ou resposta imediata por se tratar de uma conta pessoal.
- Não existe acordo de nível de serviço entre o provedor e o TJPE.

- Alguns recursos das soluções providas podem requerer liberações nem sempre possíveis de serem realizadas, pois podem causar impactos indesejáveis de segurança no ambiente (ex: liberações de rede, instalações de add-ons/plug-ins, etc.). Nestes casos não há como solicitar a disponibilização de alternativas para o provedor do serviço.
- Não existem relatórios de uso, acesso, incidentes ou outros sob o controle do TJPE. Portanto, o estabelecimento de métricas fica restrito às eventuais informações disponibilizadas pela ferramenta.

Conclusão

As soluções de uso pessoal para criação de formulário e edição de documentos na nuvem não contam com características que atendam aos requisitos legais, normativos e técnicos para sua adoção como solução corporativa pelo TJPE. Tais serviços existem para a utilização por pessoas naturais com a finalidade de apoiar suas micro atividades cotidianas. Sob a ótica da segurança da informação não há como a SETIC dar garantias sobre a integridade, confidencialidade e disponibilidade dos dados e do serviço.

Recife - 05/12/2018

Poder Judiciário de Pernambuco
Secretaria de Tecnologia da Informação e Comunicação – SETIC
Assessoria de Governança de Tecnologia da Informação e Comunicação – AGTIC
Núcleo de Segurança da Informação - NSI