Parecer sobre solicitações de usuários para instalação de software de comunicação Skype e congêneres em máquinas do TJPE

Com intuito de responder sobre eventuais solicitações de instalação ou uso do Skype e softwares congêneres por meio de ativos pertencentes ao TJPE seguem os esclarecimentos.

O Skype é um serviço de comunicação instantânea e mensagens por meio de texto, áudio e vídeo. Atualmente a Skype, criadora e proprietária do software de mesmo nome, é uma empresa pertencente à Microsoft, com sede localizada nos EUA. O software para uso dos serviços providos pela empresa pode ser instalado sem custo financeiro direto para o usuário. Entretanto, ao instalar o software, o usuário concorda automaticamente com seus termos (*http://www.skype.com/pt-br/legal/*). Considerando os termos disponibilizados pela Skype, em relação aos impactos de segurança acarretados pelo eventual uso do serviço Skype pelo Tribunal de Justiça de Pernambuco, os seguintes pontos são considerados:

- A **Skype coleta, armazena e usa todas as informações de comunicação**, como, por exemplo, mas não se restringindo a: dados de cadastro, endereçamento, localização geográfica, comunicações por *chat*, correio de voz, transmissão de vídeo, dados de tráfego, resultados de pesquisas, contatos, localização de redes *wi-fi*, dispositivos de redes *wi-fi*, dados da operadora de telefonia móvel, informações sobre dispositivo móvel, como modelo, número de série, nome do fabricante, etc.
- **Os servidores da nuvem Skype estão nos EUA** e podem ser realocados para qualquer outra posição geográfica de acordo com as necessidades da empresa. **Todas as comunicações são intermediadas por esta nuvem de servidores**.
- A Skype prevê que qualquer informação que esteja sob seu poder será:
    - **Fornecida** nos casos de obrigatoriedade legal **para autoridades jurídicas, policiais ou governamentais (atualmente informações armazenadas nos EUA podem ser solicitadas legalmente por órgãos do Executivo, sem participação do Judiciário dos EUA, por meio de *National Security Letters*, com base no *Patriot Act*)**.
    - **Fornecida** às **empresas, operadores, parceiros de prestação do serviço e/ou agentes do grupo Skype**.
- Informações de mensagens de áudio **podem ser acessadas por analistas da Skype para sua conversão em texto**, quando utilizados serviços específicos da plataforma.
- **As informações armazenadas pela Skype tornam-se ativos de propriedade da empresa**. Portanto, eles podem ser considerados como itens em transações de venda da Skype para outras entidades. Ao escolher o Skype, os usuários, conscientemente, contribuem diretamente para aumentar o valor deste ativo.
- A licença de uso dos serviços do Skype é **para a pessoa que utiliza o software** e não para a instituição, não havendo **possibilidade de relacionamento, exigências sobre os serviços ou reclamações por parte do TJPE**. Não existe nenhum contrato de prestação de serviços entre as entidades.

Os pontos acima ferem diretamente a RESOLUÇÃO Nº 349, de 04 de março de 2013 (Política de Segurança da Informação do Tribunal de Justiça de Pernambuco) que define em seu Art. 20º:

> *Art. 20 º. Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente judiciário ou das quais tiver acesso no exercício de suas atividades, **são de propriedade e/ou direito de uso exclusivo do TJPE**.*
>
> *Parágrafo único. **Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais**, dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.*

> *Art. 22. A utilização de qualquer recurso da infraestrutura de tecnologia deve ser **restrito à execução de atividades inerentes e previamente previstas para o desempenho de suas funções ou concessões formalmente divulgadas pelo TJPE**, seguindo a política de conceder apenas as permissões indispensáveis para realização das suas atividades.*

O Art 26º, especificamente, proíbe a gravação e divulgação de vídeo, imagem ou áudio sem autorização formal da instituição. Mesmo que este software viesse a ser liberado para uso, o conteúdo registrado por meio dele não estaria mais sob o controle do TJPE, mas sim da empresa Skype:

> *Art. 26. Não é permitido aos agentes judiciários tirarem fotos, capturarem imagens, som ou vídeo do ambiente compreendido no perímetro físico sob gerenciamento do TJPE ou divulgar esses materiais sem uma autorização prévia da instituição.*

Os Art 6º e Art. 7º abaixo atribuem aos agentes do Judiciário Pernambuco a responsabilidade por zelar por qualquer informação gerada, armazenada ou manuseada na execução das suas atividades. A utilização do Skype por agentes do Judiciário implica em não conformidade com estes artigos:

> *Art. 6 º Para os efeitos desta Política entende-se por classes de **agentes do Judiciário**: magistrados, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, voluntários e terceirizados que possuam um vínculo formal com o TJPE.*
>
> *Art. 7 º Cabe aos agentes do Judiciário:*
> *- Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações **a pessoas que não tenham nível de autorização suficiente**;*
> *- Não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, **por qualquer meio, informações sobre ativos ou de procedimentos do TJPE, exceto quando houver autorização prévia e formal por superior hierárquico ou de acordo com a legislação vigente para tanto**;*
> *- Não conduzir, transportar, enviar, transmitir, compartilhar ou **deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle do Tribunal sem autorização formal**;*
> ***- Proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizados**;*

Pelo exposto nos termos da Skype a utilização de seus serviços configura um meio de levar informações para fora do domínio e controle TJPE, visto que estes conteúdos são armazenados em computadores localizados em outros países. Na prática registros e conteúdo das comunicações feitas a serviço do TJPE seriam de propriedade da empresa Skype/Microsoft para utilização de acordo com diretrizes próprias ou legislações estrangeiras. É simplesmente impensável no contexto apresentado qualquer garantia de que as informações não serão utilizadas, divulgadas, compartilhadas ou transmitidas sem qualquer supervisão do Tribunal. Também fica claro que o TJPE não teria como rastrear ou auditar posteriormente caso algum evento desta natureza venha a ocorrer.

Existem também questões técnicas na utilização dos serviços providos pela Skype que impactam diretamente sobre a segurança da informação. Os seguintes pontos são relevantes:

- **O Skype pode incluir softwares e scripts de terceiros**. Isto é potencialmente perigoso, pois estaríamos permitindo softwares em nosso ambiente que não passaram por qualquer avaliação de uso ou de segurança e sequer sabemos as condições que nos submeteremos ao utilizar estes programas. Controlar isso seria inviável, pois as atualizações do Skype já incluem estes softwares, que são instalados automaticamente.
- O Skype utiliza em sua forma de comunicação um modelo distribuído, onde **um terceiro computador pode servir como ponte entre uma comunicação**. Desta forma, o conteúdo trafegado entre as duas pontas da comunicação em algum momento passará por este terceiro computador. Isto é um

artifício utilizado pelo serviço Skype para contornar ferramentas de segurança como *firewalls* e *NATs*. Este comportamento acarreta algumas implicações:
    - Ponto de fragilidade para **interceptação de comunicações**.
    - Dificuldade de gerenciamento, administração de carga e configurações de rede, visto que **o software é quem decide sobre o uso de computadores intermediários**.
- O funcionamento geral do Skype depende de uma varredura que software faz sobre o computador que está instalado e sobre o ambiente de rede que ele está funcionando. Portanto, **informações sobre o computador e a rede são consolidadas e utilizadas pela Skype.** Não há qualquer garantia que estas informações não são compartilhadas ou tratadas de forma segura.
- **O código fonte e o protocolo de comunicação utilizado pelo Skype são privados e fechados**. A empresa, através dos seus termos de uso do serviço, **não permite análises sobre o código ou protocolo** (engenharia reversa de protocolo ou código fonte, análises, etc.). O conhecimento que se tem sobre o funcionamento do Skype foi criado com base em iniciativas de engenharia reversa executadas por grupos independentes interessados nas implicações de segurança no uso do Skype. Isto é um dificultador para o monitoramento e auditoria.
- O software **não oferece controles para uso corporativo**, por exemplo, que permitam a restrição do uso pelos agentes judiciários somente para suas atividades de trabalho e com contatos pré-estabelecidos.

Não se limitando ao fato ser inviável gerenciar e auditar o uso de Skype, a impossibilidade de monitoramento deste serviço também é algo crítico. As condições expostas acima vão de encontro a RESOLUÇÃO Nº 349:

> *§ 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.*
>
> *Art. 20 º. ...*
>
> *Parágrafo único. **Todos os ativos e informações do TJPE devem ser utilizados apenas para o cumprimento das atividades profissionais**, dentro do padrão de conduta ética estabelecida pela Estrutura Normativa de Segurança da Informação do TJPE e às demais leis em vigor, respeitando os requisitos de sigilo profissional.*
>
> *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.*
>
> *Art. 27. É vedado aos agentes do judiciário acessar ou armazenar, a partir de dispositivos ou recursos de TIC do TJPE ou pessoais em seu proveito, conteúdo que caracterize atividade ilegal, que não condiga com as atividades a serem cumpridas ou que possa causar prejuízo ao bom funcionamento da infraestrutura de TIC do TJPE, a exemplo, mas não se limitando, de:*
>
> *- conteúdo ou ambientes que ponham em risco a incolumidade da segurança dos dispositivos e ativos de TIC do TJPE, tais quais sítios de internet suspeitos de conterem scripts maliciosos ou consistirem em prática de fraude, **instalação de softwares maliciosos, desconhecidos ou não homologados pelo NSI, vinculado à SETIC**;*

> *Art. 31.* ***As trocas de mensagens eletrônicas institucionais somente devem ser realizadas para fins laborais, utilizando sistemas fornecidos ou homologados pela SETIC****, mantendo vocabulário formal e condizente com a reputação esperada, evitando subjetividades e intimidades em seus conteúdos.*

Como a utilização de serviços supostamente gratuitos de armazenamento na nuvem não se dá por um relacionamento institucional entre a empresa fornecedora e o TJPE, ficando este relacionamento restrito entre a pessoa física, o usuário, e o fornecedor, não há sequer possibilidade de incluir nesta relação a exigência exposta no Art. 36:

> *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****.*

Desta forma, não existe a possibilidade de liberação deste tipo serviço para uso institucional. A recomendação do NSI é que seja identificada pelas áreas competentes da SETIC uma solução que não sofra com tantas restrições relacionadas à segurança da informação. Podendo as áreas, de ofício, contar com o apoio do NSI na escolha da ferramenta no que diz respeito aos aspectos de segurança da informação. Cabe ainda uma consulta à área de infraestrutura de TIC, em cada caso, sobre a nossa capacidade de atender ao tráfego de vídeo sem prejudicar as atividades que já dependem de nossa infraestrutura de comunicação.

Recife - 25/02/2014

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