Parecer sobre solicitações de acesso ao sistema Judwin 1° Grau do TJPE por Policiais do Centro Integrado de Inteligência de Defesa Social – CIIDS da SDS/PE

Com intuito de responder ao Ofício n° 156/2014 – GAB/SDS, encaminhado pela Secretaria de TIC do TJPE, que trata de uma solicitação de acesso ao sistema Judwin 1° Grau para policiais da Secretaria de Defesa Social, seguem as considerações técnicas.

O sistema Judwin 1° Grau é um sistema que tem por finalidade básica acompanhar a movimentação processual e armazena alguns tipos específicos de documentos relacionados aos processos judiciais. Os dados constantes no sistema são inseridos e mantidos pelos magistrados e servidores responsáveis pela tramitação processual. A possibilidade de liberação do Judwin 1° Grau para uso por policiais da SDS deve levar em consideração as seguintes questões técnicas, normativas e legais:

- **Arquitetura do sistema**: o sistema funciona sobre o modelo de arquitetura cliente servidor. Ou seja, em condições normais de uso precisa que um cliente para o sistema operacional Windows seja instalado na máquina do usuário. Isto gera um empecilho técnico para uso direto do sistema por entidades externas à rede do TJPE. Respeitando o disposto nos artigos que tratam de *least privilege* e *need to know* da Resolução Nº 349, de 04 de março de 2013 (Política de Segurança da Informação e Comunicação), considerando também que não se trata de acesso a um ambiente de rede ou acesso ao sistema operacional de uma máquina, mas sim a uma aplicação cliente servidor, a única alternativa plenamente aderente à Resolução seria por meio de uma solução de virtualização de aplicações.

  O TJPE conta com uma solução de virtualização de aplicações. Este ambiente permitiria que o Judwin 1° Grau fosse acessado externamente por uma forma de acesso já padronizada pelo TJPE, sem necessidade de instalação do aplicativo nas máquinas, garantindo a distribuição facilitada de novas versões e sem liberações de redes que poderiam implicar em riscos para a infraestrutura do TJPE. Entretanto, atualmente dois problemas incidem sobre a solução implantada no TJPE: falta de suporte em contrato e necessidade de certificados digitais ICP-Brasil de servidor atualizados para o bom funcionamento da solução. Uma solução que chegou a ser considerada nesta avaliação foi a utilização de conexão VPN. Entretanto, foi levantado que estaríamos mais sujeitos a situações onde os princípios de *least privilege* e *need to know* poderiam ser comprometidos, além de termos mais dificuldade de distribuição de novas versões.

- **Aderência a normas internas do TJPE e legislações**: todas as soluções de TIC disponibilizadas no âmbito do TJPE devem ser avaliadas sob a luz da Resolução nº 349, de 04 de março de 2013. A referida Resolução é bastante clara sobre alguns aspectos que devem ser contemplados em uma eventual solução. No seu Art. 21 está definido que o acesso aos recursos de TIC por usuários que não sejam servidores ou magistrados deve ser autorizado previamente pela Presidência. O mecanismo que supri tal autorização seria um convênio, acompanhado da lista de policiais cujo acesso seria liberado, tendo em vista que o objetivo é cooperação entre órgãos de dois poderes. Como o próprio Ofício n° 156/2014 – GAB/SDS esclarece, o convênio que existia neste sentido está expirado desde 03 de fevereiro de 2014.

  Os dispositivos que tratam de *least privilege* e *need to know* e o Art. 22 definem que o privilégio deve ser o mínimo necessário para execução, formalmente autorizadas, das atividades. Portanto, no caso desta solução, o privilégio deveria ser somente leitura. Mesmo neste caso, os Art. 11 e Art. 42 da Resolução nº 349 obrigam o TJPE a manter registro (trilhas) que permitam auditorias sobre as atividades dos usuários.

  Com relação ao segredo e sigilo dos processos (Código do Processo Civil, Código de Processo Penal, etc.), cabe ao TJPE garantir o acesso somente às partes e aos representantes. Desta forma, para esta solução, seria imprescindível que os processos com estas características fossem suprimidos, tendo sua visualização impedida.

  Finalmente, independente da solução de comunicação, de acordo Instrução de Serviço Nº 04, de 16/05/2013, os certificados a serem utilizados deveriam se emitidos sob a ICP-Brasil. Salvo no caso de impossibilidade técnica comprovada.

- **Perfis/privilégios de acesso disponíveis no sistema e trilhas de auditoria**: como explicado na seção anterior, a solução deveria disponibilizar usuários do sistema para os policiais com perfil somente leitura. Isto existe na aplicação, portanto, não seria fator de impedimento. Entretanto, quanto a supressão de processos em segredo ou sigilosos, o sistema não conta com esta funcionalidade para o perfil somente leitura. As trilhas de auditoria para o perfil em questão também não existem, portanto, precisariam ser implementadas dentro do Judwin 1º Grau. Isto poderia ser amenizado com a geração de trilhas no

ambiente de virtualização de aplicações. A solução de comunicação deveria se dar por meio de certificados digitais adquiridos para cada um dos usuários da SDS.

Considerando o exposto, o Núcleo de Segurança da Informação entende que a necessidade é legitima e deve-se trabalhar no sentido de atender os requisitos acima para que o acesso seja viabilizado. Restando como pontos impeditivos, carecendo de implementação antes de qualquer liberação de acesso:

1. Formalização da renovação do convênio
2. Implementar a supressão de processos em segredo ou sigilo
3. Ativar a geração de trilhas na solução de comunicação (futuramente implementar na aplicação)
4. Emitir e configurar os certificados digitais no ambiente de virtualização de aplicações
5. Iniciar a contratação de suporte da plataforma de virtualização de aplicações para evitar interrupções do serviço

Recife - 19/08/2014

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