PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 224, DE 9 DE OUTUBRO DE 2024

Institui a Norma Complementar para Uso Seguro de Computação em Nuvem no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT-7).

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de regular as diretrizes para uso seguro de serviços de Tecnologia da Informação e Comunicação (TIC) em nuvem (*cloud computing*);

CONSIDERANDO a Política de Segurança da Informação e Comunicação deste Tribunal, estabelecida pela Resolução Normativa TRT7 nº 5, de 3 de março de 2023;

CONSIDERANDO a Instrução Normativa nº 05, de 30 de agosto de 2021, do Gabinete de Segurança Institucional da Presidência da República,
que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

CONSIDERANDO o Acórdão do Conselho Superior da Justiça do Trabalho (CSJT) nº A-2201-66.2022.5.90.0000, que recomenda ao TRT-7 "Avaliar a recepção da IN-GSI/PR 05/2021 ou outra que a suceder, à luz da realidade fática de serviços essenciais em nuvem, por ocasião da próxima revisão/atualização do Plano de Gestão de Incidentes Cibernéticos",

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir a Norma Complementar para Uso Seguro de Computação em Nuvem no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT-7), com os seguintes objetivos:

I - fornecer diretrizes para a adoção segura de serviços de computação em nuvem, garantindo a proteção de dados, a conformidade com regulamentos e a eficiência operacional;

II - definir as funções e as responsabilidades dos(as) agentes designados(as) para o gerenciamento dos serviços de computação em nuvem;

Art. 2º Para os efeitos deste normativo, são estabelecidas as seguintes definições:

I - computação em nuvem: refere-se à entrega, por meio da Internet, de recursos de Tecnologia da Informação (TI) como serviço e sob demanda.
Os recursos podem ser servidores para as aplicações, áreas de armazenamento, bancos de dados, redes, softwares, segurança e inteligência, com definição de preço de pagamento conforme o uso. Em vez de comprar, ter e manter datacenters e servidores físicos, pode-se acessar serviços de tecnologia usando um provedor de nuvem.

II - cloud broker: empresa que atua como integrador dos serviços de computação em nuvem entre o órgão e dois ou mais provedores de serviço de nuvem. O uso de um cloud broker facilita a escolha, contratação e o gerenciamento desses serviços e ainda traz benefícios como redução de custos, maior flexibilidade e agilidade.

III - Security by Design: refere-se ao princípio de incorporar medidas de segurança desde o início do processo de design de um sistema, aplicativo ou de um produto. Em vez de adicionar segurança como uma reflexão tardia, o conceito enfatiza a integração de controles de segurança desde a concepção inicial, considerando ameaças potenciais, mitigando vulnerabilidades conhecidas e garantindo que a proteção dos dados e dos(as) usuários(as) seja uma prioridade central. Isso envolve a implementação de práticas de codificação seguras, arquiteturas resilientes, autenticação robusta, controle de acesso granular e monitoramento contínuo para detectar e responder potenciais brechas de segurança.

IV - Security by Default: refere-se ao princípio de configurar um sistema, serviço ou dispositivo com as configurações mais seguras disponíveis como configuração inicial. Isso significa que, ao ser implantado ou instalado, o sistema já está pré-configurado com medidas de segurança robustas. O sistema é projetado para operar com segurança máxima desde o momento em que é ligado pela primeira vez. Isso pode incluir configurações de firewall pré-definidas, restrições de acesso baseadas em políticas, criptografia de dados ativada por padrão, atualizações automáticas de segurança e outras práticas que reduzem significativamente a exposição a ameaças cibernéticas. O objetivo é mitigar riscos antes que possam ser explorados, garantindo que a segurança seja uma característica integrada e não opcional do sistema desde o início.

V - Infraestrutura como Serviço (IaaS): modelo de computação em nuvem que fornece aos(às) usuários(as) acesso a recursos de computação virtualizados pela internet. Isso inclui servidores virtuais, armazenamento, redes e outros recursos básicos de computação. Os(As) usuários(as) têm controle total sobre o sistema operacional e sobre os aplicativos, sendo responsáveis pela manutenção de suas próprias aplicações e de seus dados.

VI - Plataforma como Serviço(PaaS): modelo de computação em nuvem que oferece uma plataforma de desenvolvimento e operação completa, permitindo que os(as) desenvolvedores(as) construam, testem e gerenciem aplicações sem se preocuparem com a infraestrutura subjacente. Isso inclui recursos como ambiente de desenvolvimento integrado (IDE), bancos de dados, ferramentas de análise e outros serviços. Os(As) usuários(as) podem focar na criação de software, enquanto o provedor de PaaS gerencia a infraestrutura.

VII - Software como Serviço (SaaS): modelo de computação em nuvem que entrega aplicativos hospedados e gerenciados via web. Os(As) usuários(as) acessam esses aplicativos por meio de um navegador da web, geralmente pagando uma assinatura mensal ou anual. Os provedores de SaaS cuidam de toda a infraestrutura, manutenção e atualizações dos aplicativos.

CAPÍTULO II
DAS DIRETRIZES

Art. 3º A adoção de computação em nuvem deve estar contemplada na estratégia do Tribunal, que deverá relacionar as metas a serem alcançadas e os objetivos da adoção do serviço de computação em nuvem.

Art. 4º Na definição da estratégia, materializada no Plano Diretor de TIC, devem ser considerados:

I - comparação abrangente de custo (nuvem versus ambiente próprio);

II - a estrutura organizacional para sustentação da estratégia;

III - a identificação dos benefícios da mudança de paradigma;

IV - a estratégia de TIC da Justiça do Trabalho;

V - a estratégia de TIC do Poder Judiciário;

VI - a definição de mecanismo de governança, para garantir a adoção de boas práticas de segurança da informação;

VII - o processo de gerenciamento de risco, desde a fase de planejamento do projeto;

Art. 5º O Tribunal deverá prover treinamentos regulares nas tecnologias e nas práticas de segurança para os(as) servidores(as) da Secretaria de Tecnologia da Informação e Comunicação (SETIC) envolvidos(as) no planejamento, migração e na sustentação dos serviços em nuvem.

Art. 6º A contratação de serviços em nuvem, nas modalidades IaaS ou PaaS, deve ser realizada, preferencialmente, por meio de integrador (cloud broker), contemplando dois ou mais provedores de serviço de nuvem.

Art. 7º O Tribunal deverá desenvolver e testar planos de continuidade para os serviços de TI hospedados em nuvem, descrevendo os cenários de falhas ou de ataques cibernéticos e as medidas de recuperação estabelecidas.

Art. 8º O planejamento da contratação de serviços de computação em nuvem, sem prejuízo da observância da legislação aplicada, deve considerar:

I - avaliação de necessidade: identificar e documentar os requisitos específicos para serviços de computação em nuvem, incluindo aspectos de desempenho, segurança, conformidade e de custo;

II - pesquisa de mercado: realizar uma pesquisa detalhada dos provedores de serviços de nuvem, considerando suas certificações e seu histórico de segurança e conformidade com as regulamentações;

III - segurança da informação: garantir a adoção de controles rigorosos de proteção de dados, gestão de acessos, registros de operações (logs de auditoria) e de monitoramento de eventos;

IV - análise de riscos: realizar uma análise de riscos específica para identificar e mitigar possíveis vulnerabilidades associadas aos dados e aos sistemas que serão migrados para a nuvem;

V - termos contratuais: garantir que os contratos com fornecedores(as) de serviços de nuvem incluam cláusulas específicas sobre a propriedade e a proteção de dados, em especial, a garantia de conformidade com a Lei Geral de Proteção de Dados (LGPD);

VI - níveis de serviços: definir e acordar níveis de serviços que atendam às necessidades do Tribunal, incluindo tempos de resposta, disponibilidade e desempenho.

CAPÍTULO III
DAS FUNÇÕES E RESPONSABILIDADES

Art. 9º Cabe ao Comitê de Segurança da Informação e Proteção de Dados:

I - propor diretrizes para adoção segura de computação em nuvem, incluindo a revisão deste ato normativo;

II - avaliar e estabelecer, se necessário, restrições geográficas sobre onde os dados e as informações do Tribunal poderão ser armazenados;

III - definir os requisitos criptográficos mínimos para o armazenamento de dados e de informações em soluções de computação em nuvem;

Art. 10. Cabe à Presidência do Tribunal analisar as deliberações do Comitê de Segurança da Informação e Proteção de Dados quanto à adoção ou à modificação das diretrizes para o uso seguro de computação em nuvem.

Art. 11. Cabe à SETIC a implementação desta norma complementar.

Art. 12. Cabe ao Gestor de Segurança da Informação:

I - supervisionar a aplicação deste ato normativo sobre uso seguro de computação em nuvem;

II - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes.

Art. 13. Ficará a cargo da unidade responsável pela infraestrutura de TIC:

I - assegurar a contínua efetividade da comunicação com o(s) provedor(es) de serviço de nuvem para o Tribunal, de forma a garantir que os controles e os níveis de serviços acordados estejam sendo observados;

II - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios.

CAPÍTULO IV
DOS REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

Art. 14. Deverão ser observados os seguintes requisitos mínimos para adoção de soluções de computação em nuvem de forma segura, sem prejuízo dos requisitos estabelecidos pelos normativos específicos aplicáveis ao Poder Judiciário:

I - a adoção de boas práticas de segurança da informação para diminuir as vulnerabilidades, desde a fase de planejamento e projeto dos serviços digitais a serem utilizados em nuvem (security by design);

II - o modelo de segurança compartilhada, para habilitar os mecanismos de segurança pertinentes à carga de trabalho implementada (security by default), seguindo a divisão de responsabilidades entre o provedor de nuvem e o TRT-7 de acordo com o modelo de serviço da carga de trabalho implementada (IaaS, PaaS, SaaS);

III - o auto provisionamento de recursos na nuvem e ajuste de acordo com as necessidades no decorrer do tempo, de maneira automática, sem a necessidade de interação com provedor de serviços;

IV - a elasticidade na alocação e na liberação de recursos contratados dinamicamente, conforme demanda;

V - a mensuração automática de serviços para estabelecimento de níveis mínimos de serviços, otimização de recursos e, se aplicável, precificação por uso;

VI - o emprego, pelo provedor, de fortes medidas para garantir o isolamento lógico dos dados e dos recursos computacionais do Tribunal, impossibilitando o acesso por outros(as) clientes do provedor, bem como, impedir a redução de desempenho dos serviços do Tribunal em razão de carga de trabalho de outros(as) clientes;

VII - o monitoramento para assegurar a transparência no uso de recursos, o controle de uso, além de verificar inobservâncias às normas definidas e fornecer evidências, no caso de incidentes de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei;

VIII - a segurança em múltiplas camadas para proporcionar a sobreposição de controles de segurança, a fim de mitigar riscos, particularmente se houver ataque bem-sucedido em uma das camadas;

IX - a detenção, pelo TRT-7, do maior nível de privilégio de administração da nuvem pública de que fizer uso;

X - a garantia da efetiva utilização de mecanismos fortes de gerenciamento de identidade e de controle de acesso, para proteger a autenticação e a autorização de acessos, com base na política de privilégios mínimos;

XI - o registro e o monitoramento dos eventos (logs) para detectar e responder a incidentes de segurança de forma eficaz.

Art. 15. Os serviços em nuvem serão providos exclusivamente pela unidade responsável pela infraestrutura de TIC do TRT-7.

Art. 16. Este Ato entra em vigor na data de sua publicação.

Fortaleza, 9 de outubro de 2024.
DURVAL CÉSAR DE VASCONCELOS MAIA
Presidente do Tribunal