TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ
Rua Álvaro Ramos, 157 - Bairro Centro Cívico - CEP 80530-190 - Curitiba - PR - www.tjpr.jus.br

INSTRUÇÃO NORMATIVA Nº 7977132 - DGRH-DDAA

SEI!TJPR Nº 0096436-13.2021.8.16.6000
SEI!DOC Nº 7977132

INSTRUÇÃO NORMATIVA CONJUNTA Nº 111/2022 - TJPR/MPPR/DPE-PR/SESP-PR/SEJUF-PR/DETRAN-PR

Dispõe sobre o estabelecimento de requisitos formais que regulamentam a segurança das atividades de colaboração entre as instituições envolvidas no TERMO DE COOPERAÇÃO TÉCNICA nº 35/2020.

O **Tribunal de Justiça do Estado do Paraná**, o **Ministério Público do Estado do Paraná**, a **Defensoria Pública do Estado do Paraná**, a **Secretaria de Estado da Segurança Pública e Administração Penitenciária do Paraná**, a **Secretaria de Estado da Justiça, Família e Trabalho do Paraná** e o **Departamento de Trânsito do Estado do Paraná**, no uso de suas atribuições legais e,

CONSIDERANDO que a edição de ato normativo conjunto visa estabelecer requisitos formais para o trato da segurança das atividades de colaboração entabuladas pelos interessados no Termo de Cooperação Técnica nº 35/2020 (SEI!TJPR nº 0055570-02.2017.8.16.6000);

CONSIDERANDO que o princípio da segurança jurídica deve permear a legislação de modo geral;

CONSIDERANDO o disposto no expediente SEI!TJPR nº 0096436-13.2021.8.16.6000;

RESOLVEM:

Art. 1º Esta Instrução Normativa estabelece requisitos formais que regulamentam a segurança das atividades de colaboração entre as instituições envolvidas no TERMO DE

COOPERAÇÃO TÉCNICA nº 35/2020, bem como as aplicações e serviços de tecnologia provenientes da colaboração.

CAPÍTULO 1
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para melhor entendimento e menor ambiguidade do conteúdo desta instrução normativa, ficam estabelecidos os termos e expressões, referenciadas em caixa alta:

I - **INSTITUIÇÃO(ÕES):** instituições envolvidas no termo de cooperação técnica, cujas atividades relacionadas são regidas por esta instrução normativa.

II - **APLICAÇÃO(ÕES):** aplicações, sistemas e serviços desenvolvidos, provenientes das atividades de colaboração entre as INSTITUIÇÕES.

III - **INFRAESTRUTURA:** equipamentos, ativos e recursos relacionados aos ambientes necessários à hospedagem, execução e exposição das APLICAÇÕES ao público alvo, incluindo:

a) equipamentos e ambientes físicos, como salas dedicadas, computadores, roteadores, dispositivos de armazenamento e comunicação, entre outros.

b) ativos de software, como máquinas virtuais, sistemas operacionais, servidores de aplicação, plataformas de conteinerização, serviços de segurança, coleta e gravação de logs, monitoria, comunicação, entre outros.

IV - **VCS:** do inglês *Version Control System*, refere-se ao sistema de controle e armazenamento do código fonte de aplicações e sistemas de tecnologia, capaz de manter histórico completo, passível de auditoria e rastro de responsabilidades sempre que necessário.

V - **VPN:** do inglês *Virtual Private Network*, refere-se ao controle de acesso a redes de tecnologia digitais quando, não havendo exposição à Internet pública, é realizado por meio de uma *Rede Virtual Protegida* oficialmente controlada ou contratada pela INSTITUIÇÃO responsável.

VI - **2FA:** do inglês 2 *(Two) Factor Authentication*, refere-se à proteção adicional no controle de acesso a sistemas e recursos de tecnologia pela exigência de um segundo fator de autenticação, além de um primeiro comumente já utilizado, como senhas ou certificados.

VII - **INFORMAÇÕES SENSÍVEIS:** refere-se à senhas, segredos, chaves, certificados, tokens ou qualquer informação relacionada ao controle de acesso às APLICAÇÕES, recursos da INFRAESTRUTURA ou à intercomunicação com demais sistemas e serviços de tecnologia.

VIII - **OIDC:** do inglês *OpenID Connect*, refere-se ao protocolo de autenticação e autorização, atualmente usado de forma abrangente por soluções de tecnologia ao redor do mundo.

IX - **LGPD:** Lei Geral de Proteção de Dados pessoais, decretada formalmente pela Lei nº 13.709, de 14 de agosto de 2018.

X - **TLS:** do inglês *Transport Layer Security*, refere-se ao conjunto de protocolos de criptografia usados para proteger a comunicação entre redes e serviços digitais.

XI - **HTTP:** do inglês *Hypertext Transfer Protocol*, refere-se ao protocolo de alto nível, abstraído dos protocolos fundamentais de comunicação digital, usado por sistemas e serviços para transferência de conteúdo não linear, incluindo imagens, vídeos, áudio, texto, metadado, formatação, entre outros.

XII - **HTTPS:** do inglês *Hypertext Transfer Protocol Secure*, refere-se ao mesmo protocolo HTTP estendido para uso conjunto com protocolos TLS para proteger a transferência do conteúdo de ponta a ponta.

XIII - **SERVIÇOS DE ARMAZENAMENTO:** refere-se a serviços digitais utilizados para persistência, consulta e organização das informações e configurações pertinentes às APLICAÇÕES e seus usuários. Inclui soluções tradicionais ou distribuídas, como bancos de dados relacionais, não relacionais, sistemas de arquivos, serviços de indexação, serviços de compartilhamento, entre outros.

XIV - **BACKUP:** refere-se à cópia e documentação protegidas dos recursos, conteúdo e processos necessários para restauração da INFRAESTRUTURA, das APLICAÇÕES, dos SERVIÇOS DE ARMAZENAMENTO, dos dados persistidos e configurações, em caso de problemas, perdas, corrupção de dados ou desastres.

XV - **SSH:** do inglês *Secure Shell Protocol*, refere-se ao protocolo de criptografia seguro usado para operação remota de sistemas operacionais da INFRAESTRUTURA.

XVI - **SCP:** do inglês *Secure Copy Protocol*, refere-se ao protocolo de transferência de arquivos e artefatos digitais realizada de forma segura por uso conjunto com protocolo SSH.

XVII - **RSYNC:** do inglês *Remote Sync*, refere-se à ferramenta usada para sincronizar arquivos e artefatos digitais entre sistemas operacionais por meio do protocolo SSH.

XVIII - **TELNET:** do inglês *Teletype Network*, refere-se ao protocolo de comunicação digital usado para operação remota de sistemas operacionais da INFRAESTRUTURA.

XIX - **FTP:** do inglês *File Transfer Protocol*, refere-se ao protocolo usado para transferência de arquivos e artefatos digitais.

XX - **AMBIENTES DE DESENVOLVIMENTO, HOMOLOGAÇÃO, TREINAMENTO E PRODUÇÃO:** referem-se aos ativos e serviços de infraestrutura necessários para hospedagem e disponibilidade de cópias distintas das APLICAÇÕES em zonas dedicadas

para respectivo desenvolvimento, homologação integrada, treinamento e exposição definitiva ao público alvo.

Parágrafo único. Os equipamentos, ativos e recursos referenciados no inciso III deste artigo PODEM ser de propriedade e soberania das próprias INSTITUIÇÕES ou terceirizados em conformidade com as leis de contratação e licitação do Estado Brasileiro.

Art. 3º Para determinar e delimitar os diferentes níveis de cada requisito, ficam estabelecidos os significados das expressões usadas ao longo desta instrução normativa, referenciadas em caixa alta:

I - **DEVE:** Esta palavra, alternativamente usada em forma adjetiva como **OBRIGATÓRIO(A), REQUERIDO(A)** ou **EXIGIDO(A)**, indica a definição de exigências absolutas.

II - **NÃO DEVE:** Esta expressão indica a definição de **proibições absolutas**.

III - **DEVERIA:** Esta palavra, alternativamente usada como **RECOMENDA-SE** ou em forma adjetiva como RECOMENDADO(A), indica que podem haver motivos válidos e circunstâncias específicas para ignorar um requisito que é necessário. As implicações devem ser melhor entendidas e avaliadas antes de optar-se por alternativas.

IV - **NÃO DEVERIA:** Esta expressão, alternativamente usada como **NÃO SE RECOMENDA** ou em forma adjetiva como **NÃO RECOMENDADO(A)**, indica que podem haver motivos válidos e circunstâncias específicas onde uma opção diferente do necessário é aceitável ou até mesmo útil. As implicações devem ser melhor entendidas e avaliadas antes de serem incorporadas.

V - **PODE:** Esta palavra, alternativamente usada em forma adjetiva como **OPCIONAL**, indica que determinado requisito é verdadeiramente opcional, cuja ausência não trará impactos às atividades de colaboração e segurança das APLICAÇÕES, INFRAESTRUTURA e SERVIÇOS DE ARMAZENAMENTO. Tais requisitos serão ignorados ou incorporados mediante avaliação do impacto previsto na realização, entrega, implantação e sustentação das soluções.

CAPÍTULO 2
DOS REQUISITOS GERAIS

Art. 4º Cada INSTITUIÇÃO DEVE designar e alocar recursos humanos necessários ao célere andamento das atividades de colaboração.

I - DEVEM ser designados recursos humanos para as áreas de:

a) **Negócio:** para definição e esclarecimento de dúvidas das regras de negócio, acompanhamento de entregas, homologação e aprovação das APLICAÇÕES.

b) **Desenvolvimento:** para planejamento, arquitetura, desenvolvimento e sustentação de software das APLICAÇÕES.

c) **Infraestrutura:** para implantação, sustentação de ambientes, acompanhamento e apoio técnico a demais equipes responsáveis pelas APLICAÇÕES.

Parágrafo único. Conforme disponibilidade de recursos em cada INSTITUIÇÃO, o mesmo PODE ser designado a mais de uma das áreas definidas no inciso I deste artigo.

CAPÍTULO 3
DA INFRAESTRUTURA

Art. 5º DEVEM ser utilizados AMBIENTES e recursos da INFRAESTRUTURA distintos e isolados para as etapas de DESENVOLVIMENTO, HOMOLOGAÇÃO, TREINAMENTO E PRODUÇÃO.

Parágrafo único. APLICAÇÕES hospedadas em determinado ambiente, bem como seus usuários e clientes, NÃO DEVEM obter acesso cruzado, compartilhando serviços ou reutilizando recursos de outros ambientes.

Art. 6º APLICAÇÕES hospedadas em determinado ambiente DEVEM obter acesso à Internet pública através de proxy ou firewall, com devidos controles e restrições de uso.

Art. 7º O acesso direto ao AMBIENTE DE PRODUÇÃO da INFRAESTRUTURA, DEVE ser restrito às funcionalidades e finalidades oficialmente suportadas pelas APLICAÇÕES, salvo administradores da INFRAESTRUTURA e rotinas de BACKUP automatizadas.

Art. 8º RECOMENDA-SE que o acesso direto administrativo à INFRAESTRUTURA seja realizado através de protocolos reconhecidamente seguros, como SSH, SCP ou RSYNC, em favor de protocolos mais antigos, como TELNET ou FTP.

Art. 9º Alterações, atualizações e configurações diretas realizadas pelos administradores na INFRAESTRUTURA DEVEM ser controladas e formalmente documentadas, mantendo histórico passível de auditoria e rastro de responsabilidades sempre que necessário.

Art. 10. Cada INSTITUIÇÃO DEVE seguir um plano próprio de atualização tecnológica dos ativos e recursos da INFRAESTRUTURA cujo objetivo seja eliminar vulnerabilidades ou falhas de segurança.

Parágrafo único. NÃO DEVEM, por consequência do caput, utilizar ou manter em atividade plataformas, sistemas operacionais, ferramentas, pacotes, serviços, bibliotecas ou dependências em versões depreciadas e vulneráveis à falhas de segurança oficialmente reconhecidas, mitigáveis ou corrigidas pelos fornecedores.

Art. 11. RECOMENDA-SE que o acesso aos AMBIENTES DE DESENVOLVIMENTO, HOMOLOGAÇÃO E TREINAMENTO sejam restritos a redes internas e protegidas da INSTITUIÇÃO ou através de VPN, salvo necessidades específicas e formalmente Definidas.

Art. 12. RECOMENDA-SE que todos os acessos aos ambientes e recursos da INFRAESTRUTURA sejam protegidos por chaves ou certificados, em conjunto com 2FA, em favor ao controle de acesso unicamente por login e senhas.

Art. 13. As INSTITUIÇÕES DEVEM manter BACKUPS regulares da INFRAESTRUTURA.

CAPÍTULO 4
DO DESENVOLVIMENTO DE SOFTWARE

Art. 14. As INSTITUIÇÕES DEVEM manter o código fonte das APLICAÇÕES restrito através de VCS, sob controle e autoridade própria.

Parágrafo único. DEVEM, por consequência do caput, manter histórico completo de alterações e versões liberadas das APLICAÇÕES, passível de auditoria e rastro de responsabilidades sempre que necessário.

Art. 15. O Acesso ao VCS das APLICAÇÕES DEVE ser restrito:

I - às equipes de desenvolvimento e administradores relacionados.

II - às rotinas de empacotamento, implantação e automação.

Parágrafo único. RECOMENDA-SE, além da previsão do caput, a restrição de acesso através de redes internas e protegidas da INSTITUIÇÃO responsável ou através de VPN.

Art. 16. A entrega, empacotamento e implantação de versões funcionais das APLICAÇÕES DEVEM ser realizados através do VCS.

§ 1º NÃO DEVEM, por consequência do caput, ser implantadas em qualquer ambiente da INFRAESTRUTURA versões das APLICAÇÕES cujos códigos fontes não tenham sido formalmente entregues através do VCS.

§ 2º RECOMENDA-SE que os processos relacionados ao caput sejam automatizados, reduzindo a necessidade de interação e intervenção humana.

Art. 17. INFORMAÇÕES SENSÍVEIS NÃO DEVEM ser armazenadas junto ao código fonte no VCS.

CAPÍTULO 5
DA ARQUITETURA DE SOFTWARE

Art. 18. Mediante intercomunicação ou intercâmbio de documentos, arquivos e qualquer artefato digital com sistemas e serviços externos, as APLICAÇÕES DEVEM propagar o sigilo e controle de acesso provenientes de sua origem, conforme a legislação vigente relacionada.

Art. 19. Cada INSTITUIÇÃO DEVE seguir um plano próprio de atualização tecnológica das APLICAÇÕES, cujo objetivo seja eliminar vulnerabilidades e falhas de segurança.

Parágrafo único. NÃO DEVEM, por consequência do caput, utilizar ou manter em atividade:

I - linguagens de programação, frameworks, ferramentas, pacotes, serviços, bibliotecas, protocolos e dependências em versões depreciadas ou vulneráveis às falhas de segurança oficialmente reconhecidas, mitigáveis ou corrigidas pelos fornecedores.

II - algoritmos, práticas e padrões de programação que apresentam vulnerabilidades ou falhas de segurança ou que reduzem a segurança implantada por outras soluções integradas.

Art. 20. Para garantir maior segurança no uso e interoperabilidade, as APLICAÇÕES:

I - DEVEM exigir uso do protocolo HTTPS no acesso de usuários e na intercomunicação entre sistemas.

II - DEVEM exigir uso de TLS em comunicações diversas ao protocolo HTTPS.

III - DEVEM exigir uso do protocolo OIDC para situações onde autenticação e autorização de usuários e sistemas são necessárias.

IV - NÃO DEVERIAM usar soluções, protocolos e algoritmos proprietários ou fora dos padrões de mercado.

CAPÍTULO 6
DO ARMAZENAMENTO E PERSISTÊNCIA DE DADOS

Art. 21. O conteúdo resguardado pelos SERVIÇOS DE ARMAZENAMENTO no AMBIENTE DE PRODUÇÃO NÃO DEVE ser exportado ou espelhado de forma irrestrita a outros ambientes, estações de trabalho, entidades externas, outras aplicações ou ferramentas sem devido processamento, incluindo providências para:

I - redefinição ou ofuscação de INFORMAÇÕES SENSÍVEIS.

II - proteção de dados pessoais garantidos pela LGPD.

Art. 22. O Acesso direto a SERVIÇOS DE ARMAZENAMENTO DEVEM ser restritos somente às funcionalidades e finalidades oficialmente suportadas pelas APLICAÇÕES, salvo:

I - administradores dos respectivos serviços.

II - rotinas de BACKUP automatizadas.

Art. 23. Alterações diretas no conteúdo resguardado pelos SERVIÇOS DE ARMAZENAMENTO por meios estranhos às funcionalidades e finalidades oficialmente suportadas pelas APLICAÇÕES DEVEM ser controladas e formalmente documentadas em histórico, passível de auditoria e rastro de responsabilidades sempre que necessário.

Art. 24. As INSTITUIÇÕES DEVEM manter BACKUPS regulares do conteúdo armazenado e dos SERVIÇOS DE ARMAZENAMENTO.

Art. 25. Esta Instrução Normativa entrará em vigor na data de sua publicação.

Curitiba, 1º de agosto de 2022.

DES. JOSÉ LAURINDO DE SOUZA NETTO

Presidente do Tribunal de Justiça

GILBERTO GIACOIA

Procurador-Geral de Justiça

ANDRÉ RIBEIRO GIAMBERARDINO

Defensor Público-Geral

WAGNER MESQUITA DE OLIVEIRA

Secretário de Estado da Segurança Pública e Administração Penitenciária

ROGÉRIO HELIAS CARBONI

Secretário de Estado da Justiça, Família e Trabalho

ADRIANO FURTADO

Diretor-Geral do Departamento de Trânsito

Documento assinado eletronicamente por **Gilberto Giacoia**, **Usuário Externo**, em 12/08/2022, às 16:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANDRÉ RIBEIRO GIAMBERARDINO**, **Usuário Externo**, em 10/10/2022, às 15:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjpr.jus.br/validar informando o código verificador **7977132** e o código CRC **A294EF2C**.