TJAP
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

INSTRUÇÃO NORMATIVA Nº 113/2023-GP/TJAP

Regulamenta o uso Aceitável de Recursos de TIC (ferramentas institucionais do ambiente colaborativo em nuvem) no âmbito do Tribunal de Justiça do Estado do Amapá - TJAP.

O **Desembargador ADÃO JOEL GOMES DE CARVALHO**, Presidente do Tribunal de Justiça do Estado do Amapá, no uso das atribuições que lhe são conferidas pelo artigo 26, inciso XXII, do Regimento Interno do Tribunal de Justiça do Estado do Amapá - RITJAP (Resolução n.º 006/2003-TJAP), ao apreciar o Processo Administrativo nº 84898/2023;

CONSIDERANDO a Resolução CNJ n.º 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução CNJ n.º 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 1626/2023-TJAP que institui a Política de Segurança da Informação e Cibernética no âmbito do TJAP;

RESOLVE:

CAPÍTULO I
DA FINALIDADE

Art. 1º Regulamentar o uso Aceitável de Recursos de TIC (ferramentas institucionais do ambiente colaborativo em nuvem) no âmbito do Tribunal de Justiça do Amapá - TJAP.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeito deste normativo, os termos e definições são aqueles descritos no Glossário da Política de Segurança da Informação e Cibernética do TJAP, instituído pela Resolução nº 1626/2023-TJAP.

TJAP
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

CAPÍTULO III
DOS PAPÉIS E RESPONSABILIDADES

Art. 3º Compete para os assuntos de segurança da informação:

I - à Secretaria de Tecnologia da Informação e Comunicação - SETIC:

a) adquirir, instalar, gerenciar serviços e recursos em nuvem do TJAP;

b) prover os sistemas e recursos necessários para monitoramento do uso dos serviços em nuvem disponibilizados;

c) avaliar e homologar os serviços em nuvem necessários para a sustentação das operações das unidades que compõem o Tribunal Pleno;

d) elaborar procedimentos e diretrizes para o uso dos serviços em nuvem do TJAP;

e) agir de forma proativa e reativa quando identificados eventos de segurança envolvendo o uso de serviços em nuvem do TJAP.

II - à Secretaria de Gestão Pessoas - SGP e à Secretaria de Comunicação Social - SECOM apoiar o processo de divulgação, avaliação e sensibilização dos assuntos referentes à segurança da informação e cibernética;

III - aos chefes ocupantes de cargo ou função igual ou superior a CDSJ-2 divulgar e fomentar as diretrizes do uso de computadores entre seus servidores, colaboradores e estagiários;

IV - aos servidores, colaboradores e estagiários do TJAP:

a) zelar pelo uso adequado dos serviços em nuvem disponibilizados pelo TJAP;

b) comunicar à SETIC sobre eventos e incidentes envolvendo os serviços em nuvem disponibilizados;

c) cumprir com as diretrizes e orientações das normas de segurança da informação do TJAP, assim como apoiar o desenvolvimento e identificação de novas necessidades.

II - às demais unidades que compõem a estrutura do TJAP:

a) divulgar os normativos de segurança da informação para todos os seus servidores e colaboradores;

b) solicitar concessão de acesso aos serviços em nuvem para novos usuários, conforme regramento específico estabelecido.

TJAP
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

CAPÍTULO IV
DAS DISPOSIÇÕES GERAIS

Art. 4º O uso dos serviços em nuvem disponibilizados pelo TJAP está restrito às atividades exercidas por servidores, colaboradores e estagiários em seu cotidiano institucional.

§1º É vedado o uso dos serviços em nuvem de uso pessoal ou qualquer outro que não seja o disponibilizado pelo TJAP para fins laborais.

§2º Serão bloqueados os acessos a serviços de nuvem não disponibilizados pelo TJAP em todos os dispositivos corporativos, patrimoniados e ambiente de rede corporativa do Tribunal.

§3º É vedado o uso dos serviços em nuvem disponibilizados pelo TJAP, em parte ou em sua completude, para atividades que tragam ganhos e benefícios monetários e pessoais.

§4º Toda informação institucional do TJAP, que esteja em ambiente de nuvem, deve ser tratada visando as suas funções administrativas, informativas, probatórias e comunicativas, sendo vedada a apropriação dessas informações em caso de desligamento de servidores, colaboradores e estagiários.

§5º É vedado o acesso e uso das informações em ambiente de nuvem corporativa do TJAP por dispositivos pessoais e/ou não patrimoniados pelo TJAP, conforme Política de Uso Aceitável de Recursos de TIC (BYOD - dispositivos móveis pessoais) e Política de Uso Aceitável de Recursos de TIC (dispositivos institucionais).

§6º Em caso de desligamento do órgão, os dados produzidos pelo usuário durante seu tempo em exercício no TJAP pertencem ao órgão, não sendo permitido ao usuário à remoção, cópia ou alteração maliciosa dos dados ao longo do processo de desligamento.

§7º O uso dos serviços em nuvem para as atividades finalísticas do TJAP está condicionado aos recursos disponíveis conforme Mapa de Recursos Mínimos e catálogo de serviços de TI.

Art. 5º A administração dos recursos e serviços em nuvem é restrita à SETIC, por meio de seus servidores ou colaboradores de empresa contratada.

Parágrafo único. Servidores, colaboradores e estagiários das demais unidades do Tribunal não possuirão direitos de administrar recursos e/ou serviços em nuvem.

TJAP
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

Art. 6º Serão estabelecidos mecanismos de bloqueio de acessos aos serviços e recursos em nuvem em caso de ociosidade a tempo a ser definido pela equipe técnica.

Art. 7 Auditorias periódicas devem ser executadas para identificação do uso indevido dos serviços e recursos em nuvem, assim como garantir que os controles de segurança implementados estão vigentes e em conformidade com as definições institucionais.

CAPÍTULO V
DO USO DE SISTEMAS DE COMUNICAÇÃO EM NUVEM (ÁUDIO, VÍDEO E TEXTO)

Art. 8º O uso dos sistemas de comunicação é restrito para fins corporativos, sendo vedado o uso dos sistemas de comunicação para fins pessoais.

Art. 9º O uso de recursos de gravação de reuniões on-line, através dos sistemas de comunicação em nuvem, é condicionado à aprovação prévia de todos os participantes.

§1º Antes de iniciar a gravação é imperativo que haja consulta de todos os participantes, informando sobre a necessidade de registro da reunião.

§2º Ao iniciar a reunião, faz-se necessário o registro inicial da reunião informando a data e não óbice dos participantes para a gravação do evento.

§3º As gravações ficarão sob custódia do organizador da reunião para fins de registros internos.

§4º O compartilhamento da gravação para prestadores de serviços e empresas contratadas, em parte ou sua completude, está sujeita a solicitação formal, via e-mail e aprovação e registro do organizador da reunião.

Art. 10 É vedado o compartilhamento de arquivos classificados por meio de sistemas de comunicação, sem prévio registro e autorização.

§1º O compartilhamento de arquivos durante as reuniões será por compartilhamento nominal, através dos recursos dos serviços em nuvem estabelecidos.

§2º O compartilhamento deverá ter periodicidade estabelecida.

§3º As ações de salvamento local e impressão do arquivo compartilhado deverá ser inibido, a fim de garantir os atributos atômicos da confidencialidade, posse / controle e uso.

4

TJAP
TRIBUNAL DE JUSTIÇA
DO ESTADO DO AMAPÁ

CAPÍTULO VI
DO REGISTRO E MONITORAMENTO

Art. 11 Mecanismos de monitoramento dos serviços e recursos em nuvem do TJAP devem ser institucionalizados a fim de identificar e alertar sobre:

I - compartilhamentos com prestadores de serviços e empresas contratadas;

II - compartilhamentos com destinatários que não façam parte do domínio tjap.jus.br;

III - tentativas de acessos por dispositivos pessoais e/ou não patrimoniados pelos TJAP;

IV - endereço dos acessos em ambientes de rede não corporativa do TJAP;

V - acesso indevido a conteúdo, conforme diretrizes das normas de controle de acesso lógico e conectividade e acessos à Internet.

Art. 12 Registros (log) de uso e de erros ou falhas devem ser utilizados para assegurar que os problemas sejam identificados e alertados.

Art. 13 Registros de acesso devem ser mantidos por um período de 60 meses, contendo, minimamente:

I - identificação do usuário;

II - data, horário e detalhes dos acessos aos serviços e recursos em nuvem;

III - registros de tentativas de acesso a recursos e dados em nuvem aceitos e rejeitados;

IV - arquivos acessados e tipo de acesso;

V - endereço e protocolo de rede;

VI - alarmes provocados por sistema de controle de acesso.

Art. 14 Registros de log de auditoria devem ser de acesso restrito à equipe da ETIR - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Art. 15 Controles devem ser implementados para inibir a falsificação e acesso não autorizado aos registros de log.

OAB/AP [illegible]

5

TJAP
TRIBUNAL DE JUSTIÇA
DO ESTADO DO AMAPÁ

Art. 16 O backup de registros dos logs será realizado, mantendo os aspectos de segurança e criptografia dos registros de monitoramento.

CAPÍTULO VII
SANÇÕES E DAS PENALIDADES

Art. 17 Os colaboradores que não zelarem pela implementação e execução das diretrizes descritas neste normativo serão responsabilizados em caso de vazamento, total ou parcial, de informações sensíveis decorrentes de seus atos.

Art. 18 A violação ou a não aderência a este normativo será considerado um incidente de segurança da informação e acarretará a aplicação das penalidades previstas em lei.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 19 Os casos omissos serão resolvidos no âmbito do Comitê Gestor de Segurança da Informação do TJAP.

Art. 20 Esta Instrução Normativa entrará em vigor 30 dias após a data de sua publicação no Diário de Justiça Eletrônico.

Macapá - AP, 24 de novembro de 2023.

Desembargador ADÃO CARVALHO
Presidente/TJAP

CERTIDÃO DE PUBLICAÇÃO
PUBLICADO(A) NO
DJE nº 210 no dia 24/11/2023
Circulação 24/11/2023

Doc. juntado digitalmente no Processo: 2023084898 - 5, por ADRIELE NEVES DE ALMEIDA em 27/11/2023 09:42:32. A autenticidade do documento pode ser conferida no site http://sig.tjap.jus.br/scpa_control_autenticidade_documento/ informando o código verificador: **AADMOVGYKC9**