PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal Pleno Administrativo

RESOLUÇÃO Nº 349, DE 25 DE MARÇO DE 2026.

Altera e acresce dispositivos à Resolução nº 334, de 31 de julho de 2025, do Tribunal Pleno Administrativo, que dispõe sobre a Política de Segurança da Informação, no âmbito do Poder Judiciário do Estado do Acre e dá outras providências.

O **TRIBUNAL PLENO ADMINISTRATIVO**, no uso de suas atribuições legais,

CONSIDERANDO a Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO a edição da Resolução nº 334/2025, do Tribunal Pleno Administrativo, que dispõe sobre a Política de Segurança da Informação, no âmbito do Poder Judiciário do Estado do Acre e dá outras providências;

CONSIDERANDO a necessidade de constante atualização da Política de Segurança da Informação, instrumento essencial à governança e à proteção dos ativos informacionais e tecnológicos institucionais;

CONSIDERANDO o contido no processo SEI nº 0012768-80.2025.8.01.0000,

RESOLVE:

Art. 1º A Resolução nº 334, de 31 de julho de 2025, do Tribunal Pleno Administrativo, passa a vigorar com a seguinte redação:

"CAPÍTULO IV
POLÍTICA DE SENHAS E CONTROLE DE ACESSO

Art. 18. São objetivos da Política de Senhas e Controle de Acesso: (NR)

I – estabelecer diretrizes e padrões para o uso, criação, gerenciamento e troca de senhas, bem como para a definição,

concessão, revisão e revogação de acessos aos sistemas e recursos tecnológicos no âmbito do Poder Judiciário do Estado do Acre, a fim de garantir o uso seguro e controlado dos recursos computacionais, dos sistemas administrativos e judiciais deste Poder Judiciário, minimizando riscos de vazamento de dados, acessos indevidos, infecções por malwares, roubo de identidades, dentre outros riscos e incidentes cibernéticos. (NR)

.....

CAPÍTULO VI
POLÍTICA DE ACESSO À INTERNET (NR)

Art. 32. São objetivos da Política de Acesso à Internet: (NR)

I – estabelecer diretrizes e padrões para o acesso à internet por todos os usuários do Poder Judiciário do Estado do Acre, incluindo visitantes e servidores do Estado do Acre a fim de garantir a confidencialidade, integridade, disponibilidade das informações e o uso responsável dos recursos tecnológicos neste Poder Judiciário, minimizando riscos de vazamento de dados, infecções por malwares, roubo de identidades, dentre outros riscos e incidentes cibernéticos. (NR)

Art. 33. A política de acesso à internet aplica-se a todos os usuários do Poder Judiciário do Estado do Acre, incluindo visitantes, fornecedores, parceiros, prestadores de serviço e usuários internos, bem como demais pessoas autorizadas temporariamente que necessitem de acesso à internet. (NR)

Art. 34. Definições da Política de Acesso à Internet: (NR)

.....

III – usuário Interno: Servidores, colaboradores e demais integrantes do Poder Judiciário do Estado do Acre que utilizam a rede e os recursos de internet para desempenhar suas atividades funcionais e institucionais.

Art. 35. São Diretrizes da Política de Acesso à Internet : (NR)

.....

§ 3º Usuário Interno:

I – o acesso à internet pelos usuários internos será realizado por meio do login e senha do e-mail institucional, os mesmos

utilizados para fins institucionais;
II – o acesso será realizado por meio de uma rede sem fio (TJAC-CORPORATIVO), na qual ao conectar, o usuário deverá visualizar uma tela de boas–vindas (captive portal), informando que a navegação será monitorada conforme Política de Segurança da Informação do PJAC e seus anexos, e nela será necessário a inserção do login e senha o mesmo utilizado para acessos internos;

III – serão aplicadas políticas de restrição de acesso, conforme regras de segurança estabelecidas pela SUSEG.

CAPÍTULO VIII
POLÍTICA DE USO DE DISPOSITIVOS PESSOAIS

Art. 58. São objetivos da Política de Uso de Dispositivos pessoais estabelecer diretrizes para o uso de dispositivos pessoais (como notebooks, smartphones, tablets, e equipamentos similares) na rede da instituição, visando garantir a integridade, a confidencialidade e a disponibilidade das informações.

Art. 59. São diretrizes da Política de Uso de Dispositivos Pessoais:

I – é vedada a conexão de quaisquer dispositivos pessoais (como notebooks, smartphones, tablets e equipamentos similares) à rede lógica do Tribunal de Justiça do Estado do Acre, exceto nos casos previstos nos §§ 1º e 2º do art. 35, em que:

a) usuários jurisdicionados poderão conectar seus dispositivos exclusivamente à rede TJAC–VISITANTES;
b) usuários externos (prestadores de serviço, fornecedores e parceiros) poderão conectar seus dispositivos exclusivamente à rede TJAC–SERVIÇOS, quando devidamente autorizados e identificados conforme procedimentos definidos pela SUSEG.

II – a autorização excepcional para uso de dispositivos pessoais nos demais casos, para acesso a serviços internos, deverá ser formalmente solicitada à área competente, conforme detalhado no parágrafo único do Capítulo IX;
III – o usuário que descumprir esta determinação estará sujeito às medidas administrativas cabíveis, conforme as normas internas e demais dispositivos legais aplicáveis.

Art. 60. Os dispositivos pessoais devem seguir integralmente a

Política de Segurança da Informação, conforme disposto no art. 51 deste documento.

Parágrafo único. Este capítulo regula o uso de dispositivos pessoais que se conectam à rede lógica ou aos sistemas do TJAC, independentemente do tipo de porta física utilizada.

CAPÍTULO IX
POLÍTICA DE BLOQUEIO E CONTROLE DE PORTAS E MÍDIAS REMOVÍVEIS

Art. 61. Com o objetivo de prevenir incidentes de segurança da informação, como infecção por malware, vazamento de dados ou uso indevido de mídias removíveis, todas as portas USB dos equipamentos pertencentes ao TJAC serão bloqueadas por padrão.

§ 1º A liberação de portas USB para a utilização de mídias removíveis somente será permitida mediante autorização expressa da SUSEG.

§ 2º É proibida a tentativa de burlar ou alterar os mecanismos de bloqueio das portas USB implementados pela área técnica.

§ 3º O descumprimento das disposições deste artigo constituirá violação à Política de Segurança da Informação, sujeitando o responsável às medidas disciplinares previstas na legislação vigente e nas normas internas do Tribunal.

§ 4º A solicitação de liberação de que trata o inciso II do art. 59 e § 1º deste artigo, deverá ser encaminhada via processo no SEI para SUSEG, e acompanhada da assinatura do Termo de Responsabilidade para uso de recursos tecnológicos, no qual o servidor se comprometerá a utilizar a mídia ou equipamento unicamente para fins institucionais, observando as normas de segurança da informação vigentes.

CAPÍTULO X
POLÍTICA DE CONTROLE DE ACESSO PRIVILEGIADO

Art. 62. O acesso privilegiado aos sistemas, servidores, bancos de dados, dispositivos de rede e demais ativos de tecnologia da informação do Poder Judiciário do Estado do Acre será objeto de controle, auditoria e monitoramento contínuo, a fim de garantir

rastreabilidade, segregação de funções e prevenção de uso indevido.

Parágrafo único. Considera-se acesso privilegiado todo aquele que permita a execução de ações administrativas, operacionais ou de segurança capazes de alterar configurações críticas, criar ou excluir usuários, acessar dados sensíveis ou impactar na disponibilidade de serviços institucionais.

Art. 63. O gerenciamento e a monitoração de acessos privilegiados serão realizados por meio de solução de Gerenciamento de Acesso Privilegiado (PAM), que deverá assegurar, no mínimo:

I – controle centralizado de credenciais privilegiadas;
II – autenticação multifator (MFA) obrigatória para acesso ao cofre de senhas e às sessões privilegiadas;
III – gravação e armazenamento de sessões administrativas para auditoria e resposta a incidentes;
IV – registro automatizado de cada comando executado durante a sessão;
V – rotação periódica e automática de senhas privilegiadas;
VI – segregação de ambientes de produção, homologação e testes;
VII – alertas em tempo real para acessos ou atividades anômalas.

Art. 64. O acesso privilegiado somente será concedido mediante solicitação formal via SEI da Subsecretaria demandante e autorização formal da SUSEG, observando-se o princípio do menor privilégio e o tempo mínimo necessário à execução da atividade.

Parágrafo único. A solicitação deverá conter justificativa, prazo de validade, responsável técnico e sistemas envolvidos.

Art. 65. Fica vedado o uso de contas genéricas, compartilhadas ou sem identificação pessoal, devendo todo acesso privilegiado ser realizado mediante credencial individual e autenticada via PAM.

Art. 66. As credenciais privilegiadas serão rotacionadas no mínimo a cada 120 (cento e vinte) dias ou, imediatamente, em caso de suspeita de comprometimento, desligamento de colaborador, troca de função ou a critério da administração de segurança.

Art. 67. Os registros de auditoria e logs de sessões privilegiadas

deverão ser armazenados por período mínimo de 12 (doze) meses, em repositório seguro e imutável, de modo a garantir sua integridade e disponibilidade para fins de investigação ou auditoria.

Art. 68. Compete à SUSEG supervisionar a operação do PAM, definir perfis de acesso, acompanhar os relatórios de uso privilegiado e comunicar à SETIC eventuais desvios, falhas ou indícios de abuso.

Art. 69. O descumprimento das disposições deste capítulo constitui violação grave à Política de Segurança da Informação, sujeitando o responsável às medidas disciplinares e administrativas cabíveis, sem prejuízo das sanções previstas em legislação específica.

Art. 70. Os casos omissos deverão ser analisados, considerando os normativos vigentes e boas práticas de segurança da informação, pelo CGESI.

Art. 71. Esta resolução é complementar aos normativos vigentes.

Art. 72. Fica instituído o Termo de Responsabilidade para Uso de Recursos Tecnológicos, na forma do Anexo Único desta Resolução.

Parágrafo único. Tratando-se de Desembargador, caberá à Presidência do Tribunal receber os termos a que se refere este artigo.

Art. 73. Esta resolução entra em vigor na data de sua publicação.”

Art. 2º Ficam revogados os Anexos I e II da Resolução TPADM nº 334/2025.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Rio Branco-AC, 25 de março de 2026.

Desembargador **Laudivon Nogueira**
Presidente

ANEXO ÚNICO

TERMO DE RESPONSABILIDADE PARA USO DE RECURSOS TECNOLÓGICOS

Eu, [NOME COMPLETO], matrícula nº [XXXXXXX], lotado(a) no setor [NOME DO SETOR], na condição de magistrado(a), servidor(a), colaborador(a), estagiário(a), prestador(a) de serviço ou qualquer outro vínculo com o Poder Judiciário do Estado do Acre (PJAC), declaro que li, compreendi e concordo integralmente com os termos a seguir:

1. DA FINALIDADE

1.1. O presente termo tem por objetivo estabelecer as responsabilidades individuais referentes ao uso de recursos tecnológicos, acesso remoto via Rede Privada Virtual (VPN), controle de credenciais, sigilo das informações institucionais, utilização de dispositivos pessoais, bloqueio de portas e conexões, e acesso privilegiado, conforme disposto na Política de Segurança da Informação (PSI).

2. DA CONFIDENCIALIDADE DAS INFORMAÇÕES

2.1. Comprometo-me a manter o mais absoluto sigilo sobre toda e qualquer informação confidencial, sensível, estratégica ou restrita a que eu venha a ter acesso no exercício das minhas atividades, seja ela de natureza física ou digital, relativa ao PJAC, seus membros, servidores, jurisdicionados ou parceiros;

2.2. Declaro estar ciente de que a quebra de confidencialidade poderá acarretar responsabilização administrativa, civil e penal, conforme a legislação vigente e as normas internas aplicáveis.

3. DO CUMPRIMENTO DAS POLÍTICAS E NORMAS

3.1. Declaro estar ciente da existência da Política de Segurança da Informação (PSI) do PJAC e de suas políticas complementares, assumindo o compromisso de cumpri-las integralmente;

3.2. Comprometo-me a observar as instruções, procedimentos e controles técnicos definidos pela área de Tecnologia da Informação e Comunicação e pela equipe de Segurança da Informação.

4. DO USO DE RECURSOS DE TECNOLOGIA

4.1. Comprometo-me a utilizar os recursos computacionais e tecnológicos (computadores, sistemas, internet, redes, e-mails, dispositivos móveis etc.) disponibilizados pelo PJAC exclusivamente para fins institucionais e relacionados às atividades laborais;

4.2. Estou ciente que é vedado o uso de tais recursos para fins particulares, salvo exceções expressamente autorizadas;

4.3. É proibido acessar, armazenar ou transmitir conteúdo impróprio, ofensivo, ilegal ou que possa comprometer a integridade dos sistemas institucionais;

4.4. Tenho ciência de que todos os acessos e atividades poderão ser monitorados, registrados e auditados para fins de segurança e conformidade.

5. DO USO DA REDE PRIVADA VIRTUAL (VPN)

5.1. Utilizarei a VPN exclusivamente para fins profissionais, no interesse das atividades institucionais e de acordo com as permissões atribuídas ao meu perfil de acesso;

5.2. Comprometo–me a manter instalado, ativo, atualizado e devidamente licenciado um software antivírus no dispositivo que utilizarei para acesso remoto à rede institucional;

5.3. Comprometo–me a manter o firewall pessoal habilitado;

5.4. Comprometo-me a utilizar o sistema operacional original (licenciado) e com atualizações de segurança em dia.

6. DAS CREDENCIAIS DE ACESSO

6.1. Reconheço que sou inteiramente responsável pela guarda, sigilo e gerenciamento de minhas senhas de acesso aos sistemas institucionais, responsabilizando–me por eventuais acessos indevidos decorrentes do comprometimento da minha credencial;

6.2. Caso eu identifique ou suspeite de qualquer comprometimento de minhas senhas de acesso aos sistemas institucionais, comprometo–me a informar IMEDIATAMENTE à equipe responsável pela segurança da informação, para que as medidas cabíveis sejam adotadas;

6.3. Estou ciente que em caso de suspeita de violação da Política de Segurança da Informação e seus anexos, poderei ter o acesso suspenso, por prazo indeterminado, para averiguação.

7. DOS DISPOSITIVOS AUTORIZADOS

7.1**.** Concordo que somente dispositivos que atendam integralmente à Política de Segurança da Informação (PSI) poderão ser utilizados para acesso à VPN, à rede ou aos sistemas do PJAC;

7.2. Quando utilizar dispositivos pessoais, comprometo-me a seguir todas as diretrizes e requisitos técnicos estabelecidos pela equipe de Segurança da Informação, ciente de que o acesso poderá ser monitorado e controlado;

7.3**.** Declaro que utilizarei exclusivamente softwares licenciados e autorizados, sendo expressamente proibido instalar, armazenar ou executar programas não licenciados, piratas ou não aprovados pela área técnica.

8. DO USO DE DISPOSITIVOS PESSOAIS

8.1. Reconheço que o uso de dispositivos pessoais (como notebooks, smartphones, tablets, e equipamentos similares) para acessos a serviços internos, está condicionado à autorização da área técnica e ao cumprimento integral da PSI;

8.2. Comprometo-me a utilizar dispositivos pessoais apenas nos termos autorizados e exclusivamente para finalidades institucionais, observando as normas de segurança, monitoramento e rastreabilidade aplicáveis.

9. DO BLOQUEIO DE PORTAS E CONEXÕES

9.1. Estou ciente de que as portas, conexões e interfaces físicas ou lógicas dos equipamentos

institucionais poderão ser bloqueadas, restritas ou controladas para garantir a integridade e a segurança da rede;

9.2. Comprometo-me a não conectar dispositivos não autorizados às portas USB, interfaces de rede, Wi-Fi, Bluetooth ou quaisquer outras conexões que possam representar risco à segurança dos ativos institucionais.

10. DO ACESSO PRIVILEGIADO

10.1. Reconheço que acessos privilegiados a sistemas, servidores, bases de dados, dispositivos de rede e demais ativos críticos são objeto de controle rígido, auditoria e monitoramento contínuo;

10.2. Comprometo-me a não compartilhar credenciais, tokens, senhas ou quaisquer meios de autenticação, bem como a não executar ações além das permissões formalmente atribuídas ao meu perfil;

10.3. Tenho ciência de que sessões privilegiadas poderão ser registradas, auditadas e revisadas pela equipe de Segurança da Informação, conforme normas vigentes.

11. DISPOSIÇÕES FINAIS

11.1. Declaro estar ciente de que qualquer descumprimento às disposições acima poderá resultar em sanções administrativas, civis ou penais, além de perda de acesso à VPN e outras medidas previstas nas normas internas do PJAC.

Por ser verdade e para que produza os devidos efeitos, firmo o presente termo.

Local e Data: _____

Assinatura do Usuário: _____

Nome Completo: _____

Setor: _____

Documento assinado eletronicamente por **Desembargador LAUDIVON de Oliveira NOGUEIRA**, **Presidente do Tribunal**, em 26/03/2026, às 18:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjac.jus.br/verifica informando o código verificador **2360513** e o código CRC **4DEA866E**.