



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

RESOLUÇÃO Nº 334, DE 31 DE JULHO DE 2025.

Dispõe sobre a Política de Segurança da Informação, no âmbito do Poder Judiciário do Estado do Acre e dá outras providências.

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO ACRE**, por seu Pleno Administrativo, no uso das atribuições que lhe confere o art. 12 da Lei Complementar nº 221, de 30 de dezembro de 2010, combinado com o artigo 357, inciso XXVII, do Regimento Interno,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir e manter um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Poder Judiciário com integridade, confidencialidade, disponibilidade e autenticidade;

CONSIDERANDO que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade;

CONSIDERANDO que o Poder Judiciário do Acre produz e recebe informações no exercício de suas competências constitucionais, legais e regulamentares, e que tais informações devem permanecer íntegras, disponíveis, com autenticidade garantida e eventual sigilo resguardado;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes das principais normas nacionais e internacionais;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

CONSIDERANDO a Resolução CNJ 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO Resolução n. 291, de 5 de julho de 2023, que Institui a Estratégia de Tecnologia da Informação e Comunicação e a Estratégia de Segurança da Informação do Poder Judiciário do Estado do Acre;

CONSIDERANDO que o Brasil é um dos países mais afetados por ataques cibernéticos no mundo e que esses ataques podem causar prejuízos inestimáveis;

CONSIDERANDO as boas práticas em segurança preconizadas pelas Normas Técnicas ABNT NBR ISO/IEC 27001:2024, 27002:2022 e 27005:2023;

CONSIDERANDO a Lei nº 13.709/2018, Lei Geral de Proteção de Dados;

CONSIDERANDO a Lei nº 12.965/2014, Marco Civil da Internet;

CONSIDERANDO a Lei nº 12.527/2011, Lei de Acesso à Informação;

CONSIDERANDO, por fim, a deliberação do Tribunal Pleno Administrativo, no Processo Administrativo SAJ nº SAJ 0101503-89.2025.8.01.0000 e SEI nº 0003976-40.2025.8.01.0000,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer a Política de Segurança da Informação (PSI) e seus anexos no âmbito do Poder Judiciário do Estado do Acre, da qual são partes integrantes todas as normas e procedimentos complementares e afins editados pelo Poder Judiciário Estadual e que tem



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

como objetivo garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Poder Judiciário, com integridade, confidencialidade, disponibilidade e autenticidade.

Parágrafo único. A Política de Segurança da Informação deverá ser revista anualmente, ou quando necessário, em menor prazo.

Art. 2º São objetivos da Política de Segurança da Informação do Poder Judiciário do Estado do Acre:

I – estabelecer estratégias, responsabilidades e competências, com o objetivo de estruturar a segurança da informação de forma eficaz;

II – orientar e direcionar as ações necessárias para a implementação e a manutenção contínua da segurança da informação;

III – definir medidas preventivas e mitigadoras para reduzir os impactos de eventos acidentais ou intencionais, internos ou externos, que possam resultar em destruição, alteração, apropriação indevida ou divulgação não autorizada de informações, assegurando a proteção dos ativos informacionais e a preservação da imagem do Poder Judiciário Acreano;

IV – promover ações de conscientização e capacitação de pessoal, abordando a segurança da informação e a proteção de dados pessoais de maneira sistemática e consistente;

V – alinhamento às normas, regulamentações e melhores práticas relacionadas à Segurança da Informação;

VI – proteção do ambiente tecnológico do Poder Judiciário do Estado do Acre;

VII – garantir que apenas usuários autorizados tenham acesso aos recursos computacionais e dados sensíveis do Poder Judiciário do Estado do Acre.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos deste Ato aplicam-se os seguintes conceitos e definições:



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

I – Disponibilidade: garante que os dados e informações estejam disponíveis e acessíveis para os usuários autorizados quando necessário;

II – Integridade: garante a precisão e a integridade dos dados e informações, assegurando que não sejam alteradas indevidamente durante o armazenamento, o processamento ou a transmissão;

III – Confidencialidade: garante que os dados e informações estejam acessíveis exclusivamente para os usuários que têm autorização;

IV – Autenticidade: garante a autenticidade dos dados e informações, bem como a identidade das partes nas trocas de dados e informação;

V – Informações confidenciais: informações que, se divulgadas, causariam danos ou prejuízos à organização;

VI – Vulnerabilidade: fragilidade de um ativo de informação;

VII – Menor Privilégio: estabelece que um usuário, processo, sistema ou aplicação deve ter apenas os privilégios (permissões de acesso) mínimos necessários para executar suas funções específicas e nada além disso. Esse princípio reduz a superfície de ataque e os impactos de possíveis violações de segurança;

VIII – Ameaça: conjunto de eventos que tem poder para criar um incidente;

IX – Incidente: evento que representa uma ameaça de segurança para os ativos de informação;

X – Ataque Cibernético: uma tentativa de acessar, alterar ou destruir informações de forma não autorizada;

XI – Segurança da Informação: o processo de proteger as informações de uma organização de acesso, uso, divulgação, modificação ou destruição não autorizados;

XII – Usuários: magistrados(as), servidores(as), ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, empregados de empresas prestadoras de serviços terceirizados, consultores, residentes, estagiários, voluntários, visitantes entre outras pessoas que se encontrem a serviço do Poder Judiciário do Estado do Acre, que façam uso ou tenham acesso aos recursos tecnológicos, ativos de informação e de processamento no âmbito deste Poder Judiciário;

XIII – Ativos: Qualquer bem, tangível ou intangível, que tenha valor para a organização;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

XIV – Comunicação de Dados: É a transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, radiofrequência ou qualquer outro processo eletrônico ou eletromagnético ou ótico;

XV – Cultura Organizacional de Segurança da Informação: Predisposição coletiva, no âmbito do Tribunal de Justiça do Estado do Acre, favorável à adoção de procedimentos de segurança da informação, cuja consecução se dá por intermédio de um processo gradativo que abrange a sensibilização, a conscientização, a capacitação e a especialização de segmentos específicos de seus recursos humanos;

XVI – Evento de Segurança da Informação: Ocorrência identificada de um sistema, um serviço ou uma rede, que indica uma possível violação da política de segurança da informação ou falha de controles ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

XVII – Plano de Continuidade do Negócio: Visa garantir que os serviços essenciais de Tecnologia da Informação funcionem em níveis aceitáveis durante incidentes cibernéticos, e que a recuperação total dos serviços seja realizada no menor tempo possível;

XVIII – Risco: Qualificação da insegurança, por meio da combinação de probabilidade, com a gravidade de ocorrência de um evento;

XIX – Dado: Qualquer elemento definido em sua forma bruta, que, tomado isoladamente, não conduz, por si só, à compreensão de determinado fato ou determinada situação;

XX – Informação: Dados organizados e inseridos em um contexto, de maneira a propiciar elementos de análise a seu usuário, permitindo a tomada de decisões;

XXI – Gestão de Riscos de Segurança da Informação: Visa identificar, avaliar e tratar os riscos que possam comprometer a confidencialidade, integridade ou a disponibilidade da informação;

XXII – Gestão de Incidentes de Segurança da Informação: Visa assegurar que incidentes cibernéticos sejam identificados para promover a tomada de ação corretiva em tempo hábil.

Art. 4º São considerados recursos computacionais:



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

- I – computadores, notebooks, tablets, celulares, servidores físicos e virtuais, dispositivos, periféricos e demais equipamentos de tecnologia da informação e comunicação;
- II – sistemas judiciais e administrativos ou outro sistema que se assemelhe;
- III – serviços da rede de dados do PJAC;
- IV – dados armazenados e aqueles que trafegam nas redes operacionalizadas pelo PJAC.

CAPÍTULO III
PRINCÍPIOS E DIRETRIZES

Art. 5º Para os efeitos deste Ato aplicam-se os seguintes princípios:

§ 1º Os princípios oferecem consistência nas ações da organização ao longo do tempo e em diferentes situações. Eles fornecem a base ética, cultural e estratégica necessária para uma política de segurança eficaz, ajudam a evitar abordagens reativas e improvisadas à Segurança da Informação, promovendo uma mentalidade estratégica e de longo prazo. Sendo assim, os princípios são essenciais em um cenário com a dinâmica de novas ameaças cibernéticas no ambiente digital deste tribunal.

§ 2º A presente Política de Segurança da Informação tem por princípios:

- I – preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações;
- II – menor privilégio;
- III – privacidade e proteção de dados pessoais;
- IV – responsabilidade;
- V – conscientização de segurança da informação;
- VI – conformidade legal;
- VII – continuidade de negócios.

Art. 6º Para os efeitos deste Ato aplicam-se as seguintes diretrizes:



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

- a) tratamento da informação;
- b) segurança física e do ambiente;
- c) gestão de incidentes em segurança da informação;
- d) gestão de ativos;
- e) gestão do uso dos recursos operacionais e de comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
- f) controles de acesso;
- g) gestão de riscos de segurança da informação;
- h) gestão de continuidade;
- i) auditoria e conformidade;
- j) gestão de vulnerabilidades e padrões de configuração segura;
- k) gestão e monitoramento de registros de atividade (logs);
- l) desenvolvimento seguro de sistemas;
- m) uso de recursos criptográficos.

Art. 7º São destinatários desta Política de Segurança da Informação e seus anexos e estão a ela submetidos todos os usuários(as), magistrados(as), servidores(as), ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), empregados(as) de empresas prestadoras de serviços terceirizados, consultores(as), residentes, estagiários(as), voluntários(as), visitantes entre outras pessoas que se encontrem a serviço do Poder Judiciário do Estado do Acre, que façam uso ou tenham acesso aos recursos tecnológicos, ativos de informação e de processamento no âmbito deste Poder Judiciário.

Parágrafo único. Os convênios, termos de cooperação e os contratos firmados por este Poder Judiciário que envolvam utilização de recursos de tecnologia da informação devem observar as disposições deste Ato.

Art. 8º O uso adequado dos recursos de tecnologia da informação e comunicação visa a contribuir para a efetividade e a continuidade da prestação jurisdicional deste Poder Judiciário.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

§ 1º Os recursos de tecnologia da informação e comunicação, pertencentes ao Poder Judiciário e que estão disponíveis para os usuários(as), devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação e comunicação é passível de monitoramento e controle por parte do PJAC.

Art. 9º A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar a ocorrência de eventos (logs) de segurança cibernética suspeitos e divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

Art. 10. Toda informação gerada neste Poder Judiciário será classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

Art. 11. A Subsecretaria de Segurança da Informação e Infraestrutura de Tecnologia da Informação e Comunicação – SUSEG, vinculada à Secretaria de Tecnologia da Informação e Comunicação – SETIC, tem por objetivo prover soluções de segurança que agreguem valor aos serviços prestados pelo Poder Judiciário do Estado do Acre, pautadas na conscientização e no comprometimento de seus usuários para a preservação da confidencialidade, da integridade e da disponibilidade das informações, a segurança nas operações e a excelente imagem perante a sociedade.

Art. 12. As atribuições do Comitê Gestor de Segurança da Informação – CGESI, do Comitê de Crises Cibernéticas – COCRI, do Núcleo de Segurança da Informação – NUSEG e da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética – ETIR são definidas pela Resolução n. 291, de 5 de julho de 2023, que Institui a Estratégia de Tecnologia da Informação e Comunicação e a Estratégia de Segurança da Informação do Poder Judiciário do Estado do Acre e suas atualizações.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Art. 13. Incumbe à chefia imediata e superior do usuário verificar a observância desta PSI no âmbito de sua unidade, comunicando, de imediato, ao CGESI e a SUSEG deste Poder Judiciário, as irregularidades constatadas, para as providências cabíveis.

Art. 14. O não cumprimento desta Política de Segurança da Informação pode levar a violações de dados e roubo de identidade.

Art. 15. O descumprimento das normas referentes à Política de Segurança da Informação deste Poder Judiciário poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 16. Cada usuário será responsável pelo equipamento de informática utilizado, zelando e seguindo as normas determinadas de uso do equipamento, gestão de senhas pessoais e de acesso à internet.

Parágrafo único. Os computadores do PJAC conectados à rede cabeada não poderão conectar-se a nenhuma rede wifi ou qualquer outro meio de conexão externa, sem prévia autorização da SUSEG.

Art. 17. Deverão ser elaboradas em conjunto com a área de comunicação institucional do PJAC campanhas institucionais onde serão expostos os possíveis problemas de segurança e a necessidade de adequação à Política de Segurança da Informação.

CAPÍTULO IV
POLÍTICA DE SENHAS

Art. 18. São objetivos da Política de Senhas:

I – Estabelecer diretrizes e padrões para o uso, criação, gerenciamento e troca de senhas no âmbito do Poder Judiciário do Estado do Acre a fim de garantir o uso seguro dos recursos computacionais, bem como os sistemas administrativos e judiciais deste Poder



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Judiciário, minimizando riscos de vazamento de dados, infecções por *malwares*, roubo de identidades, dentre outros riscos e incidentes cibernéticos.

Art. 19. A senha para todos os recursos computacionais do Poder Judiciário do Estado do Acre é de uso pessoal e intransferível, não cabendo ao usuário compartilhá-la com terceiros.

Art. 20. Fica o usuário responsável pela guarda e gerenciamento de sua senha, responsabilizando-se por possíveis acessos indevidos mediante o comprometimento de sua credencial.

Art. 21. O usuário que identificar ou suspeitar que houve comprometimento de sua senha, deverá informar IMEDIATAMENTE o fato ocorrido à SUSEG para que sejam tomadas as medidas cabíveis.

Art. 22. É terminantemente proibido anotar senhas em papel, planilhas, bloco de notas, “post-it” ou arquivos desprotegidos de fácil acesso a terceiros.

Art. 23. Senhas nunca devem ser compartilhadas, nem mesmo com colegas de trabalho ou superiores.

Parágrafo único. Caso o compartilhamento de credenciais seja detectado, os referidos acessos serão bloqueados e os usuários serão comunicados para alteração imediata das senhas, sem prejuízo de sanções cabíveis.

Art. 24. Deverão ser adotadas por parte dos usuários boas práticas de gestão de acessos, como gerenciadores de senhas que possuam banco de dados criptografados, e nunca salvar a senha diretamente nos navegadores entre outras práticas que protegem o uso das credenciais.

Art. 25. Para a utilização dos recursos computacionais do PJAC, sempre que disponível, é obrigatório o uso da Autenticação Multifator (MFA).



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Art. 26. Para criação e troca de senhas, deverá ser observado os seguintes critérios obrigatórios:

§ 1º Critérios obrigatórios:

- I – mínimo de 12 caracteres;
- II – pelo menos uma letra maiúscula (A–Z);
- III – pelo menos uma letra minúscula (a–z);
- IV – pelo menos um número (0–9);
- V – pelo menos um caractere especial (Ex: ! @ # \$ % ^ & * () _ +).
- VI – não conter NADA referente ao nome da conta;
- VII – não ser Igual as 10 últimas senhas usadas;
- VIII – não conter acentuação;
- IX – não conter dados pessoais, como nome do usuário, data de nascimento, setor ou matrícula;
- X – evitar palavras de dicionário ou combinações comuns como “Senha123”, “Admin2024”, “Tjac@2025” Etc.

§ 2º No Caso de recursos computacionais que não se adequem aos requisitos do art. 27, § 1º, deverão ser elaborados requisitos próprios seguindo as boas práticas de segurança da informação.

Art. 27. As senhas deverão ser trocadas obrigatoriamente a cada 120 (cento e vinte) dias.

Art. 28. A alteração ou bloqueio imediato das credenciais deverão ocorrer em caso de:

- I – comprometimento, suspeito ou constatado;
- II – compartilhamento indevido;
- III – desligamento do usuário;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

IV– pela SUSEG nos casos anteriores ou justificados.

CAPÍTULO V
POLÍTICA DE MESA LIMPA

Art. 29. São objetivos da Política de Mesa Limpa:

I – Estabelecer diretrizes e padrões no âmbito do Poder Judiciário do Estado do Acre a fim de garantir a confidencialidade, integridade e disponibilidade das informações, por meio da adoção de práticas de mesa limpa e tela limpa neste Poder Judiciário, minimizando riscos de vazamento de dados, infecções por *malwares*, roubo de identidades, dentre outros riscos e incidentes cibernéticos.

Art. 30. Definições da Política de Mesa Limpa:

I – mesa limpa: prática de manter o ambiente de trabalho físico livre de documentos e materiais sensíveis quando não estiverem em uso, especialmente ao final do expediente;

II – tela limpa: prática de bloquear ou desligar dispositivos eletrônicos (computadores, notebooks, tablets etc.) quando ausente da estação de trabalho ou em inatividade;

III – informação sensível: qualquer dado que, se exposto, pode comprometer a confidencialidade, integridade, privacidade, reputação ou segurança do PJAC.

Art. 31. Diretrizes da Política de Mesa Limpa:

I – Documentos impressos com informações confidenciais ou sensíveis devem ser guardados com segurança quando não estiverem sendo utilizados;

II – É proibido deixar documentos com dados pessoais, senhas ou informações sigilosas à vista sobre mesas, impressoras ou estações de trabalho;

III – Dispositivos de armazenamento removível (pendrives, HDs externos) devem ser guardados em local seguro;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

IV – Lixeiras não devem conter documentos confidenciais sem o devido descarte seguro (ex: fragmentação ou trituração);

V – É proibido colar senhas, logins ou informações sensíveis em murais, monitores, mesas, "post-its" e similares;

VI – Estações de trabalho devem ser bloqueadas (Win+L, Ctrl+Alt+Del → Bloquear, ou equivalente) sempre que o usuário se afastar, mesmo que por curtos períodos;

VII – Os dispositivos devem ter protetores de tela com bloqueio automático ativado com tempo máximo de inatividade de 15 minutos. Casos específicos, devidamente justificados, devem ser submetidos ao CGESI para deliberação;

VIII – Sessões de sistemas críticos devem ser encerradas ao término do uso;

IX – Telas voltadas para áreas de circulação devem utilizar filtros de privacidade, se necessário;

X – Informações sensíveis exibidas em tela devem ser evitadas em ambientes públicos ou compartilhados.

CAPÍTULO VI

POLÍTICA DE ACESSO À INTERNET POR VISITANTES

Art. 32. São objetivos da Política de Acesso à Internet por Visitantes:

I – Estabelecer diretrizes e padrões para o acesso à internet por visitantes no âmbito do Poder Judiciário 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.

Art. 33. A política de acesso à internet por visitantes se aplica a todos os visitantes que necessitem de acesso à internet, incluindo fornecedores, parceiros, prestadores de serviço e demais pessoas autorizadas temporariamente.

Art. 34. Definições da Política de Acesso à Internet por Visitantes:



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

I – Usuário Jurisdicionado: Usuário que necessita de internet básica apenas para acesso aos serviços públicos;

II – Usuário Externo: Fornecedores, prestadores de serviço, parceiros e demais visitantes que necessitem utilizar a Rede do PJAC para fins de prestação de serviço (ex.: Configuração de Links, Treinamentos, Palestras e etc.).

Art. 35. São Diretrizes da Política de Acesso à Internet por visitantes:

§ 1º Usuário Jurisdicionado:

I – o acesso à internet por visitantes que são usuários jurisdicionados será realizado por meio de um cadastro no momento do primeiro acesso;

II – o acesso será realizado por meio de uma rede sem fio separada e totalmente isolada da rede institucional (TJAC–visitantes);

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

IV – este recurso destina-se a garantir a prestação jurisdicional;

V – computadores conectados à rede cabeada do PJAC não poderão conectar-se à rede TJAC–visitantes;

VI – bloqueio de conexão à VPNS e proxy externos;

VII – após 1(uma) hora de inatividade na rede o usuário jurisdicionado será desconectado.

§ 2º Usuário Externo:

I – O acesso à internet por visitantes que são usuários externos será realizado por meio de solicitação expressa do setor responsável pelo usuário externo à SUSEG;

II – O setor responsável pelo visitante usuário externo deverá informar à SUSEG com antecedência mínima de 48 horas para que haja tempo hábil de configuração e liberação de portas e serviços necessários para a prestação de serviço;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

III – Ao conectar, o usuário externo deverá visualizar uma tela de boas-vindas (captive portal) com a Política de Acesso à Internet por Visitantes, informando que a navegação será monitorada conforme Política de Segurança da Informação do Poder Judiciário do Estado do Acre e seus anexos;

IV – Ao conectar, o usuário externo deverá acessar o sistema com seu usuário e senha temporários fornecido pela SUSEG e aceitar a Política de Acesso à Internet por Visitantes;

V – O acesso será realizado por meio de uma rede sem fio separada e totalmente isolada da rede institucional (TJAC–SERVIÇOS);

VI – Serão aplicadas políticas de restrição de acesso, conforme regras de segurança estabelecidas pela SUSEG;

VII – O usuário externo deverá ser identificado (nome, empresa, e-mail e CPF) para fins de rastreabilidade;

VIII – Bloqueio de portas e protocolos não essenciais (ex.: P2P, FTP, SSH, TELNET, RDP, SMB e etc), exceto quando previamente solicitado e aprovado pela SUSEG;

IX – Bloqueio de conexão à VPNs e proxy externos, caso o usuário necessite utilizar proxy ou vpn externo, deverá utilizar meios próprios desconectado da rede do PJAC;

X – As credenciais de acesso terão validade limitada de acordo com a necessidade do usuário externo (ex.: 4 horas ou por sessão diária), sendo desativadas automaticamente após esse período;

XI – Após o tempo expirar, o usuário externo deve ser desconectado e, se necessário, solicitar novo acesso.

Art. 36. Todo o tráfego de rede será monitorado e poderá ser registrado para fins de auditoria e segurança.

Art. 37. O visitante é responsável por:

I – Cumprir integralmente a Política de Segurança da Informação do Poder Judiciário do Estado do Acre;

II – Não disseminar vírus, malware ou outros conteúdos maliciosos.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

CAPÍTULO VII
POLÍTICA DE USO DA VPN

Art. 38. São objetivos da Política de Uso da VPN:

I – Estabelecer diretrizes e padrões para o uso da VPN (Virtual Private Network), garantindo comunicação segura, acesso controlado e integridade das informações trafegadas remotamente no âmbito do Poder Judiciário do Estado do Acre a fim de garantir o uso seguro dos recursos computacionais, bem como os sistemas administrativos e judiciais deste Poder Judiciário, minimizando riscos de vazamento de dados, infecções por *malwares*, roubo de identidades, dentre outros riscos e incidentes cibernéticos.

Art. 39. São requisitos para uso da VPN:

§ 1º Autorização formal:

I – O acesso à VPN só será concedido mediante solicitação expressa do chefe imediato do setor do solicitante com a devida identificação através do Sistema Eletrônico de Informações (SEI).

§ 2º O usuário da VPN deverá assinar previamente um Termo de Responsabilidade de Acesso à VPN (anexo à PSI), comprometendo-se a:

- I – utilizar a VPN exclusivamente para fins profissionais;
- II – manter em seu dispositivo antivírus instalado, ativo, atualizado e devidamente licenciado;
- III – seguir integralmente a Política de Segurança da Informação do PJAC.

Art. 40. Fica o usuário responsável pela guarda e gerenciamento de sua senha da VPN, responsabilizando-se por possíveis acessos indevidos mediante o comprometimento de sua credencial.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Art. 41. O usuário que identificar ou suspeitar que houve comprometimento de sua senha da VPN, deverá informar imediatamente o fato ocorrido à SUSEG para que sejam tomadas as medidas cabíveis.

Art. 42. Dos dispositivos permitidos para uso da VPN:

§ 1º Dispositivos pessoais devem seguir as diretrizes da Política de Segurança da Informação.

§ 2º É obrigatório a utilização de:

I – antivírus ativo, atualizado e licenciado;

II – firewall pessoal habilitado;

III – sistema operacional licenciado e com atualizações de segurança em dia.

Art. 43. As credenciais de acesso à VPN devem seguir a Política de Senhas do PJAC.

Art. 44. O acesso à VPN deve ser protegido por autenticação multifator (MFA).

Art. 45. Certificados digitais ou tokens poderão ser exigidos em contextos mais sensíveis.

Art. 46. O tráfego deve ser criptografado com protocolos seguros (ex: IPsec, SSL/TLS).

Art. 47. Todo acesso passará por inspeção, ferramentas de monitoramento e controle.

Art. 48. O prazo de validade do acesso deve ser definido e renovado periodicamente.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Art. 49. Todas as conexões VPN são monitoradas em tempo real e seus registros armazenados por no mínimo 12 (doze) meses.

Art. 50. O usuário deverá comunicar imediatamente qualquer incidente, anomalia ou perda de dispositivo.

Art. 51. É terminantemente proibida a utilização de dispositivos que contenham quaisquer tipos de softwares piratas, craqueados, modificados ou obtidos por meios ilegais.

Art. 52. O suporte técnico ao uso da VPN será prestado exclusivamente durante o horário de expediente regular do PJAC, conforme horário previsto em normativas internas.

Art. 53. Fora do expediente, o suporte estará disponível somente para servidores portariados oficialmente para plantão no respectivo dia, mediante identificação prévia no sistema e validação com a equipe responsável.

Art. 54. O acesso à VPN não concede, por padrão, acesso a ambientes privilegiados.

Parágrafo único. Sempre que necessário o acesso remoto será concedido por meio de ferramentas específicas de controle de acesso fornecidas pela SUSEG.

Art. 55. Em caso de suspeita de violação da Política de Uso da VPN ou da Política de Segurança da Informação o usuário terá o acesso suspenso, por prazo indeterminado, para averiguação.

Art. 56. Perfis de Usuários e Restrições:

§ 1º Magistrados e Servidores:

I – deverão cumprir esta Política de Uso da VPN;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

II – terão acesso autorizado, desde que observem integralmente a Política de Segurança da Informação e seus anexos, com uso de dispositivos que sigam as regras desta PSI e a assinatura do Termo de Responsabilidade.

§ 2º Estagiários, Residentes, Voluntários:

I – o acesso à VPN é proibido, salvo exceções justificadas e aprovadas pela chefia imediata do solicitante via SEI;

II – deverão cumprir esta Política de Uso da VPN;

III – terão acesso autorizado, desde que observem integralmente a Política de Segurança da Informação e seus anexos, com uso de dispositivos que sigam as regras desta PSI e a assinatura do Termo de Responsabilidade.

§ 3º Demais casos:

I – o acesso à VPN é proibido, salvo exceções justificadas e aprovadas pela chefia imediata do solicitante via SEI;

II – deverão cumprir esta Política de Uso da VPN;

III – terão acesso autorizado, desde que observem integralmente a Política de Segurança da Informação e seus anexos, com uso de dispositivos que sigam as regras desta PSI e a assinatura do Termo de Responsabilidade.

Art. 57. Da validade do Acesso e Responsabilidade por atualização do Uso da VPN:

§ 1º Usuários em regime de teletrabalho deverão renovar a solicitação de acesso à VPN, conforme período aprovado em seu processo de teletrabalho.

§ 2º Usuários que não estiverem em regime de teletrabalho, mas que eventualmente necessitarem de acesso remoto à rede institucional, deverão renovar a solicitação a cada 6 (seis) meses, mediante nova justificativa funcional.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

§ 3º O chefe imediato e o próprio usuário são responsáveis por comunicar imediatamente à SUSEG qualquer ocorrência que implique na necessidade de desativação ou revisão do acesso à VPN, incluindo, mas não se limitando a:

- I – mudança de função ou setor;
- II – desligamento voluntário ou involuntário (exoneração, demissão, aposentadoria, etc.);
- III – cessação da necessidade de uso da VPN por mudança no regime de trabalho;
- IV – identificação de uso indevido ou infração às normas internas.

Art. 58. Os casos omissos deverão ser analisados, considerando os normativos vigentes e boas práticas de segurança da informação, pelo CGESI.

Art. 59. Esta resolução é complementar aos normativos vigentes.

Art. 60. Esta resolução entra em vigor na data de sua publicação.

Rio Branco-AC, 31 de julho de 2025.

Desembargador **Laudivon Nogueira**
Presidente



ANEXO I

TERMO DE RESPONSABILIDADE PARA USO DE VPN (REDE PRIVADA VIRTUAL)

Eu, [NOME COMPLETO], matrícula nº [XXXXXXXX], lotado(a) no setor [NOME DO SETOR], ciente das responsabilidades decorrentes do uso da Rede Privada Virtual (VPN) do PJAC, declaro que li, compreendi e concordo integralmente com os termos abaixo:

1. DO USO ADEQUADO

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

2. DAS CONDIÇÕES DE SEGURANÇA DO DISPOSITIVO

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

2.2 – Comprometo-me a manter o firewall pessoal habilitado;

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

3. DO CUMPRIMENTO DAS NORMAS

3.1 – Comprometo-me a seguir integralmente a Política de Segurança da Informação do PJAC e seus anexos, bem como todas as políticas complementares aplicáveis.

4. DAS CREDENCIAIS DE ACESSO

4.1. – Reconheço que sou inteiramente responsável pela guarda, sigilo e gerenciamento de minha senha de acesso à VPN, responsabilizando-me por eventuais acessos indevidos decorrentes do comprometimento da minha credencial.

4.2 – Caso eu identifique ou suspeite de qualquer comprometimento de minha senha da VPN, comprometo-me a informar IMEDIATAMENTE à equipe responsável pela segurança da informação, para que as medidas cabíveis sejam adotadas;



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

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

5. DOS DISPOSITIVOS AUTORIZADOS

5.1 – Concordo que somente dispositivos que cumpram a PSI poderão ser utilizados para acesso à VPN;

5.2 – Caso utilize dispositivos pessoais, comprometo-me a seguir as diretrizes estabelecidas na Política de Segurança da Informação e seus anexos, estando ciente de que o acesso será monitorado e controlado pela equipe técnica de segurança.

6. DISPOSIÇÕES FINAIS

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: _____



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

ANEXO II

TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE

Eu, [NOME COMPLETO], matrícula nº [XXXXXXX], CPF 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, declaro que li, compreendi e concordo integralmente com os termos abaixo:

1. CONFIDENCIALIDADE DAS INFORMAÇÕES:

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

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

2.1 – Declaro estar ciente da existência da Política de Segurança da Informação e seus anexos, assumindo o compromisso de cumpri-los integralmente, bem como às demais normas, procedimentos e regulamentos internos relacionados à segurança da informação.

3. USO DE RECURSOS DE TECNOLOGIA:

3.1 – Comprometo-me a utilizar os recursos computacionais e tecnológicos (computadores, sistemas, internet, redes, e-mails, dispositivos móveis, etc.) disponibilizados pelo Poder Judiciário do Estado do Acre exclusivamente para fins lícitos, legítimos e relacionados às atividades laborais, estando ciente de que:

I – É vedado o uso para fins particulares, salvo exceções previamente autorizadas;

II – É proibido acessar, armazenar ou transmitir conteúdo impróprio, ofensivo ou ilegal;

III – Os acessos e atividades serão monitorados, registrados e auditados para fins de segurança.



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

4. DAS CREDENCIAIS DE ACESSO

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

4.2 – Caso eu identifique ou suspeite de qualquer comprometimento de minha senha, comprometo-me a informar IMEDIATAMENTE à equipe responsável pela segurança da informação, para que as medidas cabíveis sejam adotadas;

4.3 – 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.

5. DOS DISPOSITIVOS AUTORIZADOS

5.1 – Concordo que somente dispositivos que cumpram a Política de Segurança da Informação e seus anexos poderão ser utilizados para acesso;

5.2 – Caso utilize dispositivos pessoais, comprometo-me a seguir as diretrizes estabelecidas na Política de Segurança da Informação e seus anexos, estando ciente de que o acesso será avaliado individualmente pela equipe técnica de segurança;

5.3 – Comprometo-me a utilizar apenas softwares devidamente licenciados e autorizados pelo PJAC, sendo expressamente proibida a instalação, uso ou cópia de programas não licenciados, piratas ou sem a devida autorização da área de Tecnologia da Informação.

6. DISPOSIÇÕES FINAIS

Declaro estar ciente de que qualquer descumprimento às disposições acima poderá resultar em sanções administrativas, civis ou penais, além de perda de acesso 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: _____



PODER JUDICIÁRIO DO ESTADO DO ACRE
Tribunal de Justiça – Tribunal Pleno Administrativo

Assinatura do Usuário: _____

Nome Completo: _____

Setor: _____