

**PORTARIA Nº 1.682, DE 22 DE SETEMBRO DE 2021.**

Processo Administrativo SEI nº 2021/000014557-00

O Desembargador **DOMINGOS JORGE CHALUB PEREIRA**, Presidente do Tribunal de Justiça do Estado do Amazonas, no exercício da competência conferida pelo art. 70, I, da Lei Complementar nº 17, de 23 de janeiro de 1997.

RESOLVE,**TORNAR SEM EFEITO** as Portarias nº 1.652 e nº 1.653, ambas de 20 de setembro de 2021.**Registre-se. Comunique-se. Publique-se.**

Gabinete da Presidência do Egrégio Tribunal de Justiça do Estado do Amazonas, em Manaus, data registrada no sistema.

*(assinado digitalmente)*Desembargador **DOMINGOS JORGE CHALUB PEREIRA**
Presidente**PORTARIA Nº 1.683, DE 22 DE SETEMBRO DE 2021.**

Processo Administrativo SEI nº 2021/000014557-00

Institui o Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD) no âmbito do Tribunal de Justiça do Estado do Amazonas - TJAM.**O Desembargador DOMINGOS JORGE CHALUB PEREIRA, Presidente do Tribunal de Justiça do Estado do Amazonas, no uso de suas atribuições legais,****CONSIDERANDO** o teor da Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei de Proteção de Dados Pessoais (LGPD);**CONSIDERANDO** a Recomendação nº 73, de 20 de agosto de 2020 do CNJ – Lei Geral de Proteção de Dados (LGPD), que recomendar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção de medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases;**CONSIDERANDO** o teor dos artigos 34º e 35º da Resolução CNJ nº 396, de 07 de junho de 2021, que revogam as Resoluções CNJ nº 360, 361, 362 de 2020, e os artigos nº 39 e 40 da Resolução 370/2021;**CONSIDERANDO** os demais assuntos pertinentes à Resolução CNJ nº 396 de 07/06/2021 para formação do Comitê; e**CONSIDERANDO** a Política de Segurança da Informação do Tribunal de Justiça do Estado do Amazonas - TJAM,**RESOLVE:****CAPÍTULO I
DISPOSIÇÕES PRELIMINARES****Art. 1º** Definir e instituir o Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD), no âmbito do Tribunal de Justiça do Amazonas (TJAM), o qual contempla:

- I** – temas relacionados à segurança da informação, de forma ampla, que sejam essenciais para segurança cibernética;
- II** – segurança física e proteção de dados pessoais e institucionais, nos aspectos relacionados à cibersegurança;
- III** – segurança física e proteção de ativos de tecnologia da informação de forma geral;
- IV** – ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;
- V** – ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades fim e administrativas do TJAM;
- VI** – ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética;
- VII** – ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética;
- VIII** – ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de tecnologia da informação e comunicação que atuam na área de segurança cibernética;
- IX** – avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do Poder Judiciário do Estado do Amazonas com as disposições da Lei nº 13.709, de 14 de agosto de 2018;
- X** – formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação;
- XI** – supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei nº 13.709, de 14 de agosto de 2018;
- XII** – prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na Lei nº 13.709, de 14 de agosto de 2018 e nas normas internas;
- XIII** – promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos.

**CAPÍTULO II
DAS DIRETRIZES DO CGSIPD**



Art. 2º O CGSIPD tem como diretrizes:

I - o aprimoramento do nível de maturidade em segurança cibernética no TJAM, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito,

II - a implementação e aplicação da Lei de Proteção de Dados no âmbito do Tribunal de Justiça do Amazonas;

III - a continuidade das atividades previstas na Portaria nº 1.933, de 23 de setembro de 2020, que instituiu o Comitê Gestor de Proteção de Dados

Art. 3º Para a concretização dos objetivos da segurança cibernética estabelecidos para o Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD), utilizar-se-á a Estratégia Nacional de Segurança Cibernética para nortear a visão, os objetivos e as ações capazes de conduzir o TJAM a um ambiente desenvolvido, resistente e seguro.

CAPÍTULO III

DA VISÃO, DAS FINALIDADES E DAS AÇÕES DO CGSIPD

Art. 4º A visão do CGSIPD consiste em promover ações que alcem o TJAM à excelência em segurança cibernética.

Art. 5º São finalidades do CGSIPD:

I – tornar o TJAM mais seguro e inclusivo no ambiente digital;

II – aumentar a resiliência às ameaças cibernéticas;

III – criar mecanismos em que o TJAM consiga estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética;

IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Art. 6º As ações devem ser estabelecidas com a finalidade de possibilitar o alcance dos objetivos e devem ser basear no estágio de maturidade geral do TJAM.

Art. 7º O TJAM deve colocar em prática as ações para o pleno alcance dos objetivos do CGSIPD.

Parágrafo único. O engajamento da alta administração do TJAM é essencial para a consecução das finalidades e das medidas de proteção ao serviço, sobretudo quando implicarem a necessidade de rápida suspensão do acesso ao público, para evitar o alastramento de ataque cibernético e conter os danos.

Art. 8º São ações do CGSIPD:

I – fortalecer as iniciativas de governança cibernética e proteção de dados;

II – elevar o nível de segurança das infraestruturas críticas;

III – estabelecer rede de cooperação do TJAM para a segurança cibernética e proteção de dados;

IV – estabelecer modelo centralizado de governança cibernética nacional.

Art. 9º Para fortalecer as ações de governança cibernética e proteção de dados, deve-se estabelecer um sistema de gestão em Segurança da Informação baseado em riscos, de acordo com a recomendação do CNJ.

Art. 10. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

I – estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais ao TJAM;

II – instituir e manter a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;

III – elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa;

IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança;

V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

VI – providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes;

VII – elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares;

VIII – elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto;

IX – adotar práticas e requisitos de segurança cibernética no desenvolvimento de novos projetos, tais como dupla verificação do acesso externo;

X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos;

XI – realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo;

XII – estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado com objetivo colaborativo.

CAPÍTULO IV

DA REDE DE COOPERAÇÃO DO TJAM NA ÁREA DE SEGURANÇA CIBERNÉTICA

Art. 11. Seguindo recomendação do CNJ, o TJAM deve integrar uma rede de cooperação na área de segurança cibernética que deve:

I – promover ambiente participativo, colaborativo e seguro no TJAM, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos;

II – estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas;

III – realizar exercícios cibernéticos com a participação de múltiplos entes;

IV – fortalecer o funcionamento do CGSIPD no TJAM;

V – aperfeiçoar a estrutura judiciária para o aprimoramento de investigações de crimes cibernéticos;

VI – incentivar a criação e a atuação de Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética no TJAM;

VII – emitir alertas e recomendações de segurança cibernética;

VIII – ampliar parceria com outros órgãos do Poder Executivo, do Poder Legislativo, do Ministério Público, do setor privado e do meio acadêmico, com vistas a elevar, de modo geral, o nível de segurança cibernética.

Parágrafo único. Para fins de cumprimento dos objetivos estabelecidos, se o TJAM detectar incidentes de segurança cibernética deverá reportá-los ao CGSIPD.



Art. 12. Compete à alta administração do TJAM realizar a governança da segurança da informação e proteção de dados, especialmente:

- I – implementar, no que lhe couber, a Política de Segurança Cibernética e proteção de dados do TJAM;
- II – destinar recursos orçamentários específicos para as ações de segurança da informação e proteção de dados;
- III – aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação e proteção de dados.

Art. 13. Ao CGSIPD caberá:

- I – assessorar a alta administração do TJAM em todas as questões relacionadas à segurança da informação e proteção de dados;
- II – propor alterações na política de segurança da informação e deliberar sobre assuntos a ela relacionados, incluindo atividades de priorização de ações e gestão de riscos de segurança;
- III – propor normas internas relativas à segurança da informação e proteção de dados;
- IV – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e proteção de dados;
- V – consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação e proteção de dados.

Parágrafo único. O CGSIPD será coordenado pela autoridade responsável pela segurança da informação no TJAM, nomeado por seu Presidente.

Art. 14. O CGSIPD deve ser uma estrutura subordinada diretamente à alta administração do TJAM e desvinculada da área de TIC;

§ 1º O titular do CGSIPD será o responsável pela gestão das atividades do CGSIPD será o gestor de segurança da informação do órgão.

§ 2º O coordenador gestor de segurança da informação terá as seguintes atribuições:

- I – instituir e gerir o Sistema de Gestão de Segurança da Informação;
- II – implementar controles internos fundamentados na gestão de riscos da segurança da informação;
- III – planejar a execução de programas, de projetos e de processos relativos à segurança da informação com as demais unidades do órgão;
- IV – implantar procedimento de tratamento e resposta a incidentes em segurança da informação;
- V – observar as normas e os procedimentos específicos aplicáveis em consonância com os princípios e as diretrizes desta Resolução e da legislação de regência.

CAPÍTULO V DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DO TJAM

Art. 15. São princípios do CGSIPD:

- I – segurança jurídica;
- II – respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção de privacidade e o acesso à informação;
- III – visão abrangente e sistêmica da segurança cibernética;
- IV – integração, cooperação e intercâmbio científico e tecnológico relacionado à segurança cibernética entre o TJAM e o meio acadêmico;
- V – educação e inovação como alicerce fundamental para o fomento da cultura em segurança cibernética;
- VI – orientação à gestão de riscos e à gestão da segurança da informação;
- VII – prevenção, tratamento e resposta a incidentes cibernéticos;
- VIII – articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação;
- IX – garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado;
- X – inviolabilidade da vida privada, da honra e da imagem das pessoas.

Art. 16. São objetivos do CGSIPD:

- I – contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio de ações de segurança cibernética, observados os direitos e as garantias fundamentais;
- II – fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética;
- III – aprimorar continuamente o arcabouço normativo relacionado à segurança cibernética;
- IV – fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;
- V – fortalecer a cultura de segurança cibernética no âmbito do TJAM;
- VI – aprimorar o nível de maturidade em segurança cibernética no TJAM;
- VII – orientar ações relacionadas às atividades de:
 - a) gestão em segurança da informação;
 - b) segurança da informação das infraestruturas críticas;
 - c) tratamento das informações com restrições de acesso;
 - d) proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com legislação específica;
 - e) prevenção, ao tratamento e à resposta a incidentes cibernéticos;
 - f) gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos;
 - g) estabelecimento dos níveis de maturidade em segurança cibernética;
 - h) estabelecimento de processo transparente de comunicação e respostas a incidentes entre o poder público e a sociedade.

Art. 17. São instrumentos do CGSIPD:

- I – a Estratégia Nacional de Segurança Cibernética do TJAM;
- II – o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do TJAM;
- III – o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do TJAM;
- IV – o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do TJAM.

§ 1º Os protocolos previstos neste artigo deverão ser revisados, sempre que necessário, por ato do Presidente do TJAM.

§ 2º Além dos protocolos previstos nesta Portaria, serão aprovados por ato do Presidente do TJAM os Manuais de Referência para o gerenciamento, controle e padrões necessários ao aperfeiçoamento da segurança cibernética.

Art. 18. Considerado o incidente como crise cibernética, o CGSIPD deverá ser acionado, nos termos do Protocolo de Gerenciamento de Incidentes e de Crises Cibernéticas.

Art. 19. O TJAM deverá estabelecer em sua Política de Segurança da Informação ações para:

- I – realizar a Gestão dos Ativos de Informação e da Política de Controle de Acesso;
- II – criar controles para o tratamento de informações com restrição de acesso;



III – promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética;

IV – estabelecer requisitos mínimos de segurança cibernética nas contratações e nos acordos que envolvam a comunicação com outros órgãos;

V – utilizar os recursos de soluções de criptografia, ampliando o uso de assinatura eletrônica, conforme legislações específicas;

VI – comunicar e articular as ações de segurança da informação com a alta administração do TJAM.

CAPÍTULO VI

DA POLÍTICA DE PROTEÇÃO DE DADOS DO TJAM

Art. 20. A aplicação desta Política de Proteção de Dados será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da LGPD, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Art. 21. O tratamento de dados pessoais pelo Tribunal de Justiça do Amazonas é realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Parágrafo único. Em atendimento a suas competências legais, o Tribunal de Justiça do Amazonas poderá, no estrito limite de suas atividades jurisdicionais, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares. Eventuais atividades que transcendam o escopo da função jurisdicional estarão sujeitas à obtenção de consentimento dos interessados.

Art. 22. O Tribunal de Justiça do Amazonas mantém contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários a suas operações, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível e ser consultada pelos interessados.

Art. 23. A responsabilidade do Tribunal de Justiça do Amazonas pelo tratamento de dados pessoais estará circunscrita ao dever de se ater ao exercício de sua competência legal e institucional e de empregar boas práticas de governança e de segurança.

Art. 24. O Tribunal de Justiça do Amazonas zela para que o Titular do dado pessoal possa usufruir dos direitos assegurados pelos artigos 18 e 19 da LGPD, aos quais a presente Política se reporta, por remissão.

Art. 25. O Tribunal de Justiça do Amazonas é o Controlador dos dados pessoais por ele tratados, nos termos das suas competências legal e institucional.

Art. 26. O Tribunal de Justiça do Amazonas pode, a qualquer tempo, requisitar informações acerca dos dados pessoais confiados a seus fornecedores. Os provedores de tais serviços serão considerados Operadores e deverão aderir a esta Política, além de cumprir os deveres legais e contratuais respectivos, dentre os quais se incluirão, mas não se limitarão aos seguintes:

I - assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais requeridas pelo TJAM.

II - apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

III - manter os registros de tratamento de dados pessoais que realizar;

IV - seguir fielmente as diretrizes e instruções transmitidas pelo TJAM;

V - facultar acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade respectiva e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição ao TJAM, mediante solicitação;

VI - permitir a realização de auditorias, incluindo inspeções do TJAM ou de auditor independente autorizado por ele autorizado, e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII - auxiliar, em toda providência que estiver ao seu alcance, no atendimento pelo TJAM de obrigações perante Titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII - comunicar formalmente e de imediato ao TJAM a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

IX - descartar de forma irrecuperável, ou devolver para o TJAM, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Art. 27. O Encarregado do Tribunal de Justiça do Amazonas será nomeado pela Presidência e observará todas as competências previstas no artigo 41 da Lei Geral de Proteção de Dados.

Parágrafo único. Os dados do Encarregado serão divulgados no sítio eletrônico do TJAM.

Art. 28. O Encarregado deverá contar com apoio efetivo deste para o adequado desempenho de suas funções.

Art. 29. A proteção de dados pessoais de magistrados e de servidores deverá observar as condições determinadas pelo Conselho Nacional de Justiça, pelo Conselho Nacional de Proteção de Dados Pessoais e pela Autoridade Nacional de Proteção de Dados, na forma da legislação e regulamentação vigentes.

CAPÍTULO VII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 30. A EASTJAM e a SETIC devem providenciar a disponibilização de curso autoinstrucional de capacitação para os integrantes da CGSIPD acerca da Lei Geral de Proteção de Dados.

Art. 31. A EASTJAM, ouvido o Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD), deverá publicar campanhas permanentes e periódicas para conscientizar os magistrados e servidores acerca da legislação de proteção de dados, com a disponibilização de manuais com orientações e, ainda, a oferta de cursos de capacitação.

Art. 32. Esta Portaria entra em vigor na data de sua publicação, revogada a Portaria nº 1.933, de 23 de setembro de 2020, que instituiu o Comitê Gestor de Proteção de Dados, bem como as demais disposições em contrário.

Registre-se. Comunique-se. Publique-se.

Gabinete da Presidência do Egrégio Tribunal de Justiça do Estado do Amazonas, em Manaus, data registrada no sistema.

(assinado digitalmente)

Desembargador **DOMINGOS JORGE CHALUB PEREIRA**
Presidente

**PORTARIA Nº 1.684, DE 22 DE SETEMBRO DE 2021.**

Processo Administrativo SEI nº 2021/000014557-00

Designa os membros do Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD) no âmbito do Tribunal de Justiça do Estado do Amazonas - TJAM.

O Desembargador DOMINGOS JORGE CHALUB PEREIRA, Presidente do Tribunal de Justiça do Estado do Amazonas, no uso de suas atribuições legais,

CONSIDERANDO o teor da Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Recomendação nº 73, de 20 de agosto de 2020 do CNJ – Lei Geral de Proteção de Dados (LGPD), que recomendar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção de medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases;

CONSIDERANDO o teor dos artigos 34º e 35º da Resolução CNJ nº 396 de 07/06/2021, que revogam as Resoluções CNJ nºs 360, 361, 362 de 2020, e os artigos nºs 39 e 40 da Resolução 370/2021;

CONSIDERANDO os dados do processo SEI nº 2021/000012200-00, bem como os demais assuntos pertinentes à Resolução CNJ nº 396 de 07/06/2021 para formação do Comitê;

CONSIDERANDO a Política de Segurança da Informação do Tribunal de Justiça do Estado do Amazonas - TJAM; e

CONSIDERANDO a instituição do Comitê Gestor de Segurança da Informação e Proteção de Dados do TJAM,

RESOLVE:

Art. 1º Designar os seguintes membros para compor o Comitê Gestor de Segurança da Informação e Proteção de Dados (CGSIPD), no âmbito do Tribunal de Justiça do Amazonas (TJAM):

I - Desembargador Délcio Luís Santos, Coordenador;

II - Dr. Jorsenildo Dourado do Nascimento, Juiz de Direito Auxiliar da Presidência, como Encarregado do TJAM;

III - Dra. Vanessa Leite Mota, Juíza de Direito Auxiliar da Corregedoria Geral de Justiça;

IV - o Secretário-Geral de Administração do TJAM;

V - o Secretário-Geral de Justiça do TJAM;

VI - o Secretário de Tecnologia da Informação e Comunicação do TJAM;

VII - a Secretária de Planejamento do TJAM;

VIII - a Secretária de Gestão de Pessoas do TJAM;

IX - Cel. George Alexandre Fonseca Feitosa, da Assistência Militar do TJAM;

X - o Gerente do Arquivo Judiciário;

XI - o Diretor de Infraestrutura de TIC da SETIC;

XII - Sr. Eduardo Gonçalves Pinheiro Junior, Coordenador SAJ;

XIII - Sr. Rodrigo dos Santos Marinho, Coordenador PROJUDI;

XIV - Sr. Sebastião Alberto Mousse Neto – SETIC;

XV - o Assessor de Segurança da Informação e Proteção de Dados da SETIC;

XVI - o Coordenador da Ouvidoria do TJAM;

XVII - o Diretor da Divisão de Contratos e Convênios da SECOP;

XVIII - o Secretário-Geral e Executivo da ESMAM;

XIX - o Coordenador acadêmico da EASTJAM;

XX - o Sr. Edivam de Lucena Nascimento Junior, Secretário do Comitê.

Parágrafo único. Fica atribuída ao senhor Edivam de Lucena Nascimento Junior. Secretário do Comitê Gestor de Segurança da Informação e Proteção de Dados - CGSIPD, a gratificação prevista no art. 6º, §1º da Resolução TJAM nº 09/2021, no valor de 15% (quinze por cento) sobre o vencimento PJ-DAS III.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Registre-se. Comunique-se. Publique-se.

Gabinete da Presidência do Egrégio Tribunal de Justiça do Estado do Amazonas, em Manaus, data registrada no sistema.

(assinado digitalmente)

Desembargador **DOMINGOS JORGE CHALUB PEREIRA**

Presidente