SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO N. 899, DE 12 DE SETEMBRO DE 2025

Institui a Política de Segurança da Informação e Comunicação (POSIC), no âmbito da Universidade Federal do Pará (UFPA), e revoga a Resolução nº 836, de 16 de dezembro de 2021.

O REITOR DA UNIVERSIDADE FEDERAL DO PARÁ, no uso das atribuições que lhe conferem o Estatuto e o Regimento Geral, em cumprimento à decisão da Colenda Câmara de Legislação e Normas e do Egrégio Conselho Universitário, em Reunião Extraordinária realizada em 12.09.2025, e em conformidade com os autos do Processo n. 030214/2025 – UFPA, procedentes do Centro de Tecnologia da Informação e Comunicação (CTIC), e, ainda,

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 27001:2013; Norma Técnica ABNT NBR ISO/IEC 27002:2013; Lei nº 12.527, de 18 de novembro de 2011 - Regula o acesso às informações; Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e sua alteração vigente; Lei nº 13.853 de 8 de julho de 2019; Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Decreto nº 11.856/2023, Instruções Normativas nº 01/2008/GSI/PR e nº 3/2021/GSI/PR,promulga a seguinte

R E S O L U Ç Ã O :

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação (POSIC), no âmbito da Universidade Federal do Pará (UFPA), constituída com um conjunto de objetivos, princípios, diretrizes, controles e responsabilidades, para garantir a segurança da informação e dos dados institucionais da UFPA, conforme o anexo (páginas 2 - 14), que é parte integrante e inseparável desta Resolução e revoga a Resolução nº 836, de 16 de dezembro de 2021.

Art. 2º Esta Resolução entra em vigor na data de sua aprovação.

Reitoria da Universidade Federal do Pará, em 12 de setembro de 2025.

GILMAR PEREIRA DA SILVA
Reitor
Presidente do Conselho Universitário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

CAPÍTULO I

DOS OBJETIVOS

Art. 1º Instituir diretrizes e princípios da Política de Segurança da Informação e Comunicação, armazenadas ou transmitidas em meio digital, no âmbito da Universidade Federal do Pará (UFPA), com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que suportam os objetivos estratégicos desta Universidade, e a proteção de dados pessoais e dados pessoais sensíveis, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Parágrafo único. A Política de Segurança da Informação e Comunicação doravante será chamada de POSIC.

Art. 2º Esta POSIC e suas normas complementares aplicam-se a todas as Unidades e Subunidades vinculadas à UFPA, bem como aos servidores, alunos, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação da UFPA, independente da forma que a informação esteja armazenada.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3. São estabelecidos os seguintes conceitos e definições para esta POSIC:

I – acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação da Universidade, seja de forma lógica (sistemas e dados) ou física (instalações dos equipamentos), desde que autorizado e controlado, podendo ser concedido com diferentes níveis de privilégios, de acordo com as necessidades e responsabilidades de cada usuário ou unidade, e devendo ser registrado e monitorado para fins de auditoria e investigação de incidentes de segurança;

II – ameaça: conjunto de fatores externos ou internos, intencionais ou não intencionais, que representam uma causa potencial de um incidente indesejado, podendo resultar em dano para os sistemas, infraestrutura e a imagem da Universidade, como ataques cibernéticos, desastres naturais, erros humanos, entre outros, com diferentes níveis de impacto, desde a interrupção de serviços até a perda de dados confidenciais;

III – ativo: qualquer bem, tangível ou intangível, que possua valor para a Universidade, computadores, servidores, equipamentos de laboratório, equipamentos do data center, equipamentos da infraestrutura de rede de dados e voz, entre outros. Os ativos devem ser protegidos de acordo com seu valor para a UFPA e os riscos a que estão expostos, e podem ser classificados em categorias de acordo com seu nível de criticidade e confidencialidade;

IV – ativos de Informação: os meios de armazenamento, transmissão e processamento de informações, incluindo dados de pesquisa, de alunos e servidores, os sistemas de informação, base de dados, documentos digitais e físicos, meios de armazenamento, entre outros, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V – autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, sistema, órgão ou entidade, garantindo a verificação da origem e integridade da informação, e relacionada ao conceito de não repúdio;

VI – Comitê de Segurança da Informação e Comunicação: grupo multidisciplinar composto por representantes de diferentes áreas da Universidade, com a responsabilidade de: propor, analisar, monitorar e promover ações de segurança da informação na Universidade;

VII – confidencialidade: propriedade de que a informação sensível ou sigilosa não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados, podendo ser garantida por meio de mecanismos como criptografia, controle de acesso e classificação de informações;

VIII – continuidade de negócios: capacidade estratégica e tática da Universidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação críticos para as atividades essenciais, de forma a manter suas operações em um nível aceitável, previamente definido, por meio da elaboração e implementação de planos de contingência e recuperação de desastres, da realização de testes e simulações periódicas, e da comunicação eficaz com as partes interessadas;

IX – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso físico (a instalações e equipamentos) ou lógico (a sistemas e dados), baseado no princípio do menor privilégio, por meio de mecanismos de autenticação, autorização e controle de acesso físico, acompanhado de registro e monitoramento das atividades dos usuários, para fins de auditoria e investigação de

incidentes de segurança;

X – controles de segurança: conjunto de políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, de natureza administrativa, técnica, de gestão ou legal, utilizados para proteger os ativos de informação da Universidade contra ameaças e vulnerabilidades;

XI – custodiante: responsável por armazenar, preservar e proteger as informações que não lhe pertencem, mas que estão sob sua custódia, garantindo a disponibilidade das informações para os usuários autorizados, mantendo um inventário das informações sob sua custódia e cumprindo as políticas e normas de segurança da informação da Universidade, podendo a custódia ser temporária ou permanente;

XII – disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizados, de forma oportuna e confiável, garantindo a continuidade das atividades da Universidade, por meio de mecanismos como sistemas de backup e recuperação de dados, servidores redundantes e planos de contingência e recuperação de desastres, e cuja interrupção pode ter diferentes níveis de impacto, desde a indisponibilidade de serviços até a paralisação de atividades críticas;

XIII – evento: ocorrência identificada em um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação, falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação, classificados em diferentes categorias, como eventos de segurança, eventos de rede e eventos de sistema, sendo monitorados e registrados para fins de detecção de incidentes de segurança e análise de comportamento, como tentativas de acesso não autorizado, falhas de autenticação, detecção de malware, alterações não autorizadas em arquivos ou configurações;

XIV – gestão de riscos de segurança da informação e comunicação: conjunto de processos contínuos e interativos que permite identificar, analisar e avaliar os riscos a que estão sujeitos os ativos de informação da Universidade;

XV – Gestão de Segurança da Informação e Comunicação (GSIC): conjunto integrado de ações e métodos para proteger os ativos de informação da Universidade. Engloba a gestão de riscos, a continuidade do negócio, o tratamento de incidentes, a segurança cibernética, conformidade legal e segurança organizacional, além de promover uma forte cultura de segurança da informação. A GSIC se aplica a todos os processos institucionais, desde o planejamento estratégico até as operações diárias, transcendendo a mera proteção de sistemas e tecnologia da informação e comunicação;

XVI – gestor de segurança da informação e comunicação: profissional responsável por planejar, coordenar e executar as ações de segurança da informação e comunicação no âmbito da Universidade, incluindo a elaboração e implementação de políticas e normas, a gestão de riscos, o tratamento de incidentes, a promoção da conscientização e a monitorização do cumprimento das políticas, sendo o ponto focal em questões de segurança da informação e segurança cibernética;

XVII – incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação, redes de computadores, dados armazenados em mídias físicas ou digitais, documentos confidenciais, informações verbais ou pessoas, ataques de *malwares*, vazamento de dados, acesso não autorizado a sistemas, perda ou roubo de equipamentos com dados confidenciais, ataques de *phishing* e engenharia social, e uso indevido de credenciais, podendo ter diferentes níveis de impacto, desde a interrupção de serviços até a perda de dados confidenciais e danos à reputação da Universidade, devendo os incidentes serem classificados de acordo com a sua gravidade;

XVIII – integridade: propriedade de que a informação, os sistemas e os processos não foram modificados ou destruídos de maneira não autorizada ou acidental, podendo ser comprometida por erros humanos, falhas de hardware ou software, e ataques cibernéticos;

XIX – nível de segurança adequado: definido para cada tipo de informação e sistema, com base em sua criticidade, sensibilidade e requisitos legais, estabelecendo os controles de segurança mínimos necessários para proteger os ativos de informação da Universidade;

XX – terceirizado/a: pessoa física ou jurídica, não integrante do quadro de pessoal da Universidade, envolvida no desenvolvimento de atividades temporárias ou eventuais, exclusivamente para o interesse do serviço público, que poderá receber credencial especial de acesso, precedida de análise e autorização formal, como consultores externos, auditores e empresas de contratadas, sendo responsável por cumprir as políticas e normas de segurança da informação da UFPA;

XXI – proprietário da informação: pessoa física ou unidade organizacional que produz ou gerencia a informação, sendo responsável por classificá-la de acordo com seu nível de sensibilidade e criticidade, definir os direitos de acesso, aprovar ou negar solicitações de acesso, garantir a integridade e a disponibilidade, e definir o tempo de retenção da informação;

XXII – comprometimento da segurança da informação: ação ou omissão, intencional ou acidental, que resulta no comprometimento da confidencialidade, integridade ou disponibilidade da informação, podendo ocorrer em diferentes níveis, desde um incidente

isolado até um ataque cibernético de grande escala, como vazamento de dados, acesso não autorizado a sistemas, ataques de *malwares*, *phishing* e a perda ou roubo de equipamentos com dados confidenciais;

XXIII – recursos de TIC: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, incluindo: aplicações, banco de dados, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade, infraestrutura, dispositivos móveis, equipamentos de videoconferência, sistemas de armazenamento em nuvem e equipamentos do data center institucional, que devem ser protegidos contra ameaças e vulnerabilidades, de acordo com as políticas e normas de segurança da informação da Universidade e gerenciados ao longo de todo o seu ciclo de vida, desde a aquisição até o descarte;

XXIV – usuário: pessoa física ou unidade organizacional que utilizam os ativos de informação e recursos de TIC da Universidade, devendo ser identificados e autenticados de forma inequívoca, e tendo seus acessos revogados quando não possuírem mais vínculo institucional, sendo responsáveis por proteger os ativos de informação a que têm acesso e por cumprir as políticas e normas de segurança da informação da UFPA, com suas atividades sendo registradas para fins de auditoria e investigação de incidentes de segurança;

XXV – vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para os sistemas da Universidade, como falhas de software, configurações incorretas de sistemas, falta de atualizações de segurança, fraquezas em controles de acesso e falta de conscientização dos usuários, podendo ser exploradas por ameaças para causar danos, com diferentes níveis de impacto, desde a interrupção de serviços até a perda de dados confidenciais e danos à reputação da UFPA;

XXVI – Lei Geral de Proteção de Dados (LGPD): instituída pela Lei nº 13.709, de 14 de agosto de 2018, e alterada pela Lei nº 13.853, de 8 de julho de 2019, estabelece regras para o tratamento de dados pessoais, tanto em meios digitais quanto físicos, por pessoas físicas e jurídica, de direito público e privado. Seu principal objetivo é proteger os direitos de liberdade, privacidade e o livre desenvolvimento da personalidade dos indivíduos. Além disso, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e regulamentar o cumprimento da lei;

XXVII – CSIRT: Grupo técnico composto por servidores com expertise em segurança da informação, segurança cibernética, redes e sistemas, responsável por monitorar, analisar, responder e tratar incidentes de segurança computacional na Universidade;

XXVIII – computação em nuvem: termo que define os serviços computacionais

(hardware e/ou software), como Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS), hospedados em provedores externos à infraestrutura física da Universidade e acessados a partir da Internet;

XXIX – computação móvel: termo que define um paradigma computacional que permite o acesso à Internet e a serviços de TIC, independentemente da localização do usuário.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º Esta POSIC é fundamentada nos seguintes princípios, que orientam todas as ações e decisões relacionadas à segurança da informação na Universidade:

I – menor privilégio: conceder aos usuários e sistemas apenas o acesso mínimo necessário para a realização de suas funções;

II – separação de função: separar as responsabilidades de planejamento, execução e controle para prevenir o uso indevido de ativos e ativos de informação;

III – auditoria: registrar e monitorar todos os eventos relevantes nos sistemas e processos, permitindo a rastreabilidade das ações;

IV – mínima dependência de segredos: implementar controles de segurança que sejam eficazes mesmo que suas características sejam conhecidas;

V – controles automáticos: priorizar a utilização de controles de segurança automatizados, reduzindo a dependência de intervenção humana;

VI – resiliência: projetar sistemas e processos capazes de resistir e se recuperar de incidentes e desastres;

VII – defesa em profundidade: utilizar múltiplas camadas de segurança para proteger os ativos, de modo que a falha de uma camada não comprometa a segurança geral;

VIII – exceção aprovada: permitir exceções à POSIC somente com a aprovação do Comitê de Segurança da Informação e Comunicação e do Comitê de Governança Digital (ou equivalente);

IX – procedimentos de segurança emergenciais: Estabelecer controles alternativos para manter a segurança em situações excepcionais;

X – confidencialidade: assegurar que o acesso à informação seja restrito a usuários autorizados;

XI – integridade: garantir a precisão e a completude da informação em todas as suas formas;

XII – disponibilidade: manter a informação e os sistemas acessíveis quando necessário para as operações da Universidade;

XIII – conformidade: assegurar que todas as práticas de segurança da informação estejam em conformidade com as leis e regulamentações aplicáveis.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5º As diretrizes de Segurança da Informação e Comunicação (SIC) devem considerar, prioritariamente, os objetivos estratégicos, os requisitos legais, a estrutura e a finalidade da UFPA.

Art. 6º Os investimentos associados à gestão da SIC devem ser proporcionais ao valor dos ativos de informação que se deseja proteger.

Art. 7º A gestão de SIC deve fornecer o suporte necessário para a tomada de decisões, a gestão de conhecimento e a alocação eficiente de recursos, contribuindo para o alcance dos objetivos estratégicos da Universidade e a otimização dos investimentos.

Art. 8º Os instrumentos e procedimentos de SIC da Universidade devem ser elaborados com base em normas e padrões de mercado reconhecidos como referência em gestão e governança de Segurança da Informação e Comunicação.

CAPÍTULO V

GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 9º Os ativos de informação são essenciais para o alcance dos objetivos estratégicos da Universidade. Para garantir sua proteção adequada, devem ser implementadas ações de segurança específicas, com níveis de proteção variando de acordo com a criticidade de cada ativo.

Art. 10. Para prevenir incidentes de segurança que possam prejudicar a imagem da Universidade e interromper suas operações, os ativos de informação devem ser protegidos contra divulgação não autorizada, modificação, remoção ou destruição, independentemente do meio em que se encontrem.

Art. 11. A conscientização, capacitação e sensibilização periódica dos usuários que acessam os ativos de informação e utilizam os recursos de TIC da Universidade são fundamentais para garantir o entendimento e a prática efetiva da SIC.

Art. 12. Os processos e atividades que sustentam os serviços críticos da Universidade devem ser protegidos para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Parágrafo único. Os ativos de informação da Universidade podem estar localizados na infraestrutura de rede institucional, em seu data center principal, em unidades com capacidade técnica de hospedagem ou serem disponibilizados e acessados por meio de computação em nuvem. Ambas as formas de localização devem estar em conformidade com a Lei Geral de Proteção de Dados (LGPD).

CAPÍTULO VI

GESTÃO DE RISCOS

Art. 13. Para reduzir vulnerabilidades, prevenir ameaças, minimizar a exposição a riscos e mitigar os impactos nos ativos da Universidade, deverá ser implementado um processo de gestão de riscos que inclua: identificação, análise, avaliação, priorização, tratamento, comunicação e monitoramento de riscos da SIC.

Art. 14. Com base na legislação vigente, deverá ser elaborado e mantido um Plano de Gestão de Riscos de SIC, que deverá conter: lista das ameaças mais prováveis e suas possíveis ocorrências, classificação dos riscos por nível de impacto e probabilidade e alternativas para mitigá-los.

CAPÍTULO VII

GESTÃO DE OPERAÇÕES E COMUNICAÇÃO

Art. 15. A segurança e o bom funcionamento dos recursos de processamento da informação são essenciais para o alcance dos objetivos da Universidade. Portanto, devem ser implementadas ações para garantir a operação segura e correta desses recursos.

Art. 16. As interfaces com terceiros representam importantes canais de informação, mas também podem expor a Universidade a riscos significativos se não forem gerenciadas adequadamente. Para minimizar esses riscos, o gerenciamento de serviços terceirizados deve garantir a segurança da informação e a entrega dos serviços em níveis apropriados.

Art. 17. A troca de informações, tanto interna quanto externa, deve ser regulamentada para manter um nível adequado de segurança, protegendo as informações confidenciais e sensíveis da Universidade.

Art. 18. Para detectar atividades não autorizadas o mais breve possível, as operações devem ser monitoradas e verificadas de forma adequada, implementando mecanismos de registro e auditoria.

CAPÍTULO VIII

CONTROLE DE ACESSOS

Art. 19. Para prevenir incidentes de segurança, devem ser estabelecidas normas e procedimentos que garantam o controle de acesso às informações e instalações da Universidade.

Art. 20. A concordância com os termos desta POSIC, é uma condição necessária para o acesso aos ativos de informação da Universidade.

Art. 21. Considerando a importância da computação móvel e do trabalho remoto para as atividades da Universidade e os potenciais riscos de SIC associados a esses ambientes, devem ser estabelecidas normas e procedimentos para garantir a segurança da informação dos ativos de informação e recursos de TIC.

Art. 22. Deve ser definido plano de controle de acesso que estabeleça procedimentos para a identificação dos ativos de informação, tanto físicos quanto de *softwares* com acesso controlado, assim como a identificação dos usuários que devem ter privilégio de acesso às áreas físicas protegidas contra o acesso de pessoas não autorizadas.

CAPÍTULO IX

GESTÃO DE INCIDENTES E DE CONTINUIDADE DO NEGÓCIO

Art. 23. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e tratados de forma oportuna e eficaz, para garantir a continuidade das atividades da Universidade e minimizar o impacto sobre seus objetivos estratégicos.

Art. 24. A interrupção das atividades da Universidade pode levar à suspensão de serviços críticos e causar danos à sua imagem. Portanto, devem ser estabelecidas normas e procedimentos para a Gestão de Continuidade do Negócio, com o objetivo de minimizar os impactos de eventos que causem indisponibilidade dos serviços, recuperar ativos de

informação perdidos e implementar ações de prevenção, resposta e recuperação.

Art. 25. A Universidade deve estabelecer um grupo técnico para o tratamento, resposta e prevenção de incidentes de segurança computacional, em conformidade com a Norma Complementar nº 05/IN01/DSIC/GSIPR, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais nos órgãos e entidades da APF.

CAPÍTULO X

CONSONÂNCIA E RESPONSABILIDADES

Art. 26. O Comitê de Segurança da Informação e Comunicação deve realizar verificações de conformidade periódicas para avaliar o cumprimento desta Política de Segurança.

Art. 27. Os controles da SIC devem ser analisados criticamente e verificados regularmente, com base em políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos padrão de mercado reconhecidos.

Art. 28. Devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da administração pública federal, de forma a obter o absoluto cumprimento destes instrumentos legais e normativos.

Art. 29. O Comitê de Governança Digital é o responsável por fornecer a orientação e o apoio necessários às ações de segurança da informação e comunicação, em consonância com os objetivos estratégicos, as leis e regulamentos aplicáveis.

Art. 30. Os demais gestores da Universidade são responsáveis por garantir o cumprimento das diretrizes desta política em suas respectivas áreas de atuação.

Art. 31. Todos os que têm acesso aos ativos de informação e recursos de TIC da Universidade são responsáveis por manter níveis adequados de segurança da informação, de acordo com esta política e suas normas complementares.

CAPÍTULO XI

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 32. O Comitê de SIC terá as seguintes atribuições mínimas:

I – assessorar o Comitê de Governança Digital na implementação das ações da SIC;

II – criar grupos de trabalho para tratar de temas específicos relacionados à SIC e propor soluções;

III – propor alterações na POSIC;

IV – propor normas e procedimentos relativos à Segurança da Informação e Comunicação.

Art. 33. O Comitê de SIC será a instância competente para esclarecer dúvidas e tomar decisões sobre assuntos relacionados à POSIC desta Universidade.

CAPÍTULO XII

GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 34. O Gestor de SIC da Universidade será o Coordenador do Comitê de Segurança da Informação e Comunicação e terá como atribuições mínimas:

I – promover a cultura de segurança da informação e comunicação na Universidade;

II – acompanhar a investigação e a avaliação de incidentes de segurança, propondo medidas corretivas e preventivas;

III – propor a alocação de recursos necessários para as ações de Segurança da Informação e Comunicação da Universidade;

IV – realizar e acompanhar estudos sobre novas tecnologias e seus possíveis impactos na segurança da informação e comunicação da Universidade;

V – propor normas e procedimentos relativos à Segurança da Informação e Comunicação da Universidade;

VI – coordenar a gestão de riscos de Segurança da Informação e Comunicação da Universidade;

VII – coordenar a criação, implementação e manutenção da infraestrutura necessária para as Equipes de Tratamento e Resposta a Incidentes de Segurança (ETRIS ou CSIRT) da Universidade;

VIII – responder às solicitações sobre SIC encaminhadas pelo Governo Federal;

IX – buscar apoio para prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETRIS (CSIRT) da Universidade.

CAPÍTULO XIII

PROPRIETÁRIO E CUSTODIANTES DOS ATIVOS DE INFORMAÇÃO

Art. 35. Os proprietários e custodiantes dos ativos de informação são diretamente responsáveis por garantir os níveis adequados de segurança desses ativos, implementando os controles necessários para proteger a confidencialidade, integridade e disponibilidade das informações.

CAPÍTULO XIV

PENALIDADES, ATUALIZAÇÕES E VIGÊNCIAS

Art. 36. O descumprimento desta POSIC poderá resultar em sanções civis, penais e administrativas, conforme previsto na legislação vigente, aplicáveis de forma isolada ou cumulativa.

Art. 37. Será instaurado um processo disciplinar específico para apurar as ações que configurem violação das diretrizes estabelecidas nesta POSIC.

Art. 38. Esta POSIC e seus documentos complementares serão revisados e atualizados, preferencialmente a dois anos, ou sempre que ocorrerem mudanças significativas que impactem a segurança da informação na Universidade.

CAPÍTULO XV

DISPOSIÇÕES GERAIS

Art. 39. Esta POSIC e suas normas e procedimentos associados devem ser amplamente divulgados para garantir que todos compreendam suas responsabilidades e ajam de acordo com seus preceitos.

Art. 40. Para fortalecer e expandir o alcance da Política de Segurança da Informação e Comunicação (POSIC) da UFPA, o Comitê de Governança Digital deve atualizar ou desenvolver instrumentos normativos, adaptados às necessidades específicas de cada área de atuação, como:

I – gestão de ativos de TIC;

II – gestão de serviços de TIC;

III – backup e restauração de dados institucionais;

IV – desenvolvimento de Software;

V – hospedagem de soluções de TIC;

VI – utilização do e-mail institucional;

VII – utilização e acesso aos recursos de TIC;

VIII – controle de acesso aos ativos de informação;

IX – serviços de TIC em nuvens computacionais;

X – gestão da segurança da informação e comunicação;

XI – gestão de continuidade de negócio de TIC;

XII – gestão de incidentes de TIC;

XIII – gestão de risco de TIC;

XIV – gestão de mudanças;

XV – gestão de configuração;

XVI – privacidade e proteção de dados;

XVII – plano de adequação a LGPD;

XVIII – plano de dados abertos.

Art. 41. Os casos omissos ou não previstos nesta política serão tratados pelo Comitê de Governança Digital.

Art. 42. Esta Política de Segurança da Informação e Comunicação entra em vigor na data de sua publicação.