Ministério da Educação
Universidade Federal do Cariri
Comitê de Governança

ATO DECISÓRIO CG N.o 01, DE 10 DE FEVEREIRO DE 2026

Aprova a Política de Segurança da Informação (POSIN) da UFCA.

O **PRESIDENTE DO COMITÊ DE GOVERNANÇA DA UNIVERSIDADE FEDERAL DO CARIRI - UFCA**, no uso da competência que lhe confere o Decreto Presidencial de 1º de junho de 2023, publicado no Diário Oficial da União, no dia 02 de junho de 2023, seção 2, página 1, e tendo em vista o que deliberou o Comitê de Governança - CG em sua Reunião Ordinária, em 10 de fevereiro de 2026, na forma do que dispõe o art. 8 do Regimento Interno do Comitê de Governança, resolve:

Art. 1º Aprovar a Política de Segurança da Informação - POSIN da Universidade Federal do Cariri — UFCA, nos termos do anexo a este Ato Decisório.

Art. 2º Este Ato Decisório entra em vigor nesta data.

ASSINADO DIGITALMENTE
SILVERIO DE PAIVA FREITAS JUNIOR
A conformidade com a assinatura pode ser verificada em:
https://serpro.gov.br/assinador-digital
Serpro

Documento assinado digitalmente
SILVÉRIO DE PAIVA FREITAS JÚNIOR
Presidente do Comitê de Governança

ANEXO

- ANEXO - DOCUMENTO: Política de Segurança da Informação (POSIN).

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
COMITÊ DE GOVERNANÇA

MINUTA DE POLÍTICA DE SEGURANÇA Nº XX/COMITÊ DE GOVERNANÇA, DE XX DE XXXX DE 2025

Dispõe sobre a Política de Segurança da Informação (POSIN) da Universidade Federal do Cariri — UFCA.

O REITOR, NO EXERCÍCIO DA PRESIDÊNCIA DO COMITÊ DE GOVERNANÇA, DA UNIVERSIDADE FEDERAL DO CARIRI, Silvério de Paiva Freitas Jr., no uso da competência que lhe confere a Portaria n° 229, de 21 de junho de 2019, combinada com o Inciso III, do Art. 25, do Estatuto em vigor da UFCA;

RESOLVE:

Atualizar a Política de Segurança da Informação (PSI) da Universidade Federal do Cariri — UFCA, doravante denominada (POSIN).

Fica revogada a resolução anterior (Resolução Nº86 / CONSUNI, de 21 de novembro de 2019).

Fica valendo, a partir da data da publicação, a nova POSIN.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação (POSIN) da Universidade Federal do Cariri (UFCA) representa o compromisso institucional com a proteção dos ativos de informação responsáveis por seu armazenamento, processamento ou transporte, sejam eles físicos, digitais ou humanos, sob sua propriedade e/ou guarda.

Parágrafo único. Esta política será complementada por: normas, processos, metodologias, procedimentos e controles a serem adotados para a gestão de segurança da informação e privacidade de dados, considerando os requisitos legais, processos organizacionais, planos institucionais e estrutura organizacional da UFCA.

Art. 2º São objetivos da POSIN:

I - estabelecer princípios e diretrizes a fim de proteger ativos de informação mantidos, gerados, tratados ou recebidos;

II - estabelecer orientações gerais de segurança da informação que contribuam para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III - estabelecer competências e responsabilidades quanto à segurança da informação;

IV - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação; e

V - promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da UFCA.

CAPÍTULO II
DAS REFERÊNCIAS SOBRE SEGURANÇA DA INFORMAÇÃO

Art. 3º Para o planejamento da gestão da segurança da informação, cabe a UFCA observar, sem prejuízo das demais normas em vigor:

I - Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação;

II - Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

III - Decreto nº 12.573, de 4 de agosto de 2025, que institui a Estratégia Nacional de Cibersegurança;

IV - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

V - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

VI - Portaria GSI/PR nº 93, de 18 de outubro de 2021 que dispõe sobre o glossário de segurança da informação da administração pública federal;

VII - Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, que dispõe o Programa de Privacidade e Segurança da Informação 2.0;

VIII - Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD);

IX - Lei Nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI);

X - demais leis, decretos, resoluções, portarias e instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República ou órgão equivalente.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições, que não estão elencados no glossário de segurança da informação:

I - alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal direta ou indireta;

II - controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

III - diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas; e

IV - usuário: pessoa física ou jurídica, seja servidor público, estudante, prestador de serviços, fornecedor, estagiário, voluntário habilitado pela administração para acessar os ativos de informação da UFCA.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 5º A POSIN da UFCA é orientada pelos princípios da administração pública e, adicionalmente, pelos seguintes valores:

I - criticidade: grau de importância de uma informação para a continuidade das atividades institucionais;

II - responsabilidade: cumprimento das normas de segurança da informação;

III - ciência: conhecimento das diretrizes que asseguram a execução segura das atribuições;

IV - ética: respeito aos direitos e interesses legítimos dos usuários da informação; e

V - proporcionalidade: adequação das ações de segurança ao valor do ativo e ao entendimento administrativo.

Art. 6º Para os serviços, recursos e informações gerenciados na infraestrutura de Tecnologia da Informação da UFCA, aplicam-se ainda os preceitos básicos da segurança da informação: *integridade, confidencialidade, disponibilidade, autenticidade* e *irretratabilidade*.

Art. 7º As ações de segurança da informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da UFCA;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da UFCA;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV - visar à prevenção da ocorrência de incidentes.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 8° As diretrizes gerais constituem os pilares da gestão de segurança da informação na UFCA, norteando a elaboração de normas, planos, procedimentos, metodologias, ações e controles que garantam o cumprimento dos princípios de segurança da informação desta POSIN.

I - a UFCA deve utilizar os guias metodológicos que serão disponibilizados pelo Gabinete de Segurança Institucional da Presidência da República ou órgão equivalente em seu sítio eletrônico, para fins de implementação de ações relacionadas à gestão da segurança da informação;

II - a alta administração deve demonstrar seu compromisso com a segurança da informação por meio do apoio ativo, da definição clara de atribuições e da responsabilização dos envolvidos;

III - a POSIN deve estar alinhada aos objetivos estratégicos, processos, requisitos legais, planos institucionais e estrutura organizacional da UFCA;

IV - um plano de gestão de segurança da informação deve ser definido juntamente com um orçamento adequado para a implementação das ações relacionadas à segurança da informação;

V - o uso dos meios e recursos de tecnologia da informação disponibilizados pela UFCA para acesso, guarda ou encaminhamento de material discriminatório, malicioso, antiético ou ilegal é expressamente proibido; e

VI - usuário pode ser responsabilizado pelos prejuízos decorrentes do descumprimento das disposições desta POSIN ou de normas complementares.

CAPÍTULO VI

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 9º A Gestão de Segurança da Informação (GSI) envolve um conjunto contínuo de processos destinados a proteger os ativos de informação, acompanhar a evolução tecnológica e mitigar os riscos que possam comprometer os objetivos estratégicos da UFCA.

Parágrafo único. Todos os processos apresentados neste capítulo, bem como suas respectivas políticas, planos e procedimentos complementares, devem ser formalmente estabelecidos, documentados, implementados, comunicados aos envolvidos e continuamente revisados.

Seção I

Do Tratamento da Informação

Art. 10 O tratamento da informação deve abranger todo o seu ciclo de vida, desde a criação até o descarte seguro, por meio de controles técnicos e procedimentos adequados para cada fase.

§ 1º A informação deve ser classificada, manuseada e armazenada de acordo com seu nível de sensibilidade e criticidade, garantindo que o acesso seja concedido com base no princípio do menor privilégio.

§ 2º A troca de informações com entidades externas deve ser formalizada por meio de acordos que garantam a manutenção do nível de segurança exigido pela UFCA.

§ 3º O tratamento de dados pessoais deve seguir as diretrizes da Lei Geral de Proteção de Dados (LGPD) e demais normas vigentes, cabendo ao Encarregado pelo Tratamento de Dados recomendar as medidas de segurança necessárias para sua proteção.

§ 4º Todos os usuários que manipulem ou tenham acesso a informações identificadas como reservadas sob custódia ou propriedade da UFCA devem garantir a confidencialidade e o sigilo destas informações, adotando comportamento seguro e discreto, evitando expô-las em ambientes sociais e particulares, ou através de impressão, transmissão/compartilhamento digital e transporte físico para fora das instalações da UFCA sem autorização formal.

Seção II

Da Segurança Física e do Ambiente

Art. 11 As instalações e os equipamentos que processam ou armazenam informações críticas devem ser protegidos contra acesso não autorizado, danos e interferências.

Parágrafo único. Áreas de acesso restrito, como *Data Centers*, devem ser protegidas por controles físicos eficazes que assegurem o acesso exclusivamente a pessoas formalmente autorizadas.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 12 O processo de gestão de incidentes visa à rápida identificação, análise, contenção e resposta a eventos adversos, minimizando o impacto nas atividades da instituição.

§ 1º O processo deve contemplar, no mínimo, as seguintes fases:

I - triagem;

II - detecção e análise de incidentes;

III - contenção, erradicação e recuperação;

IV – atividades pós-incidentes.

§ 2º Uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) deverá ser mantida, com membros devidamente capacitados para coordenar as atividades de resposta a incidentes.

Seção IV

Da Gestão de Ativos

Art. 13 Os ativos de informação (*softwares*, bancos de dados, equipamentos, serviços, etc.) devem ser inventariados, classificados e protegidos de forma proporcional ao seu valor e criticidade para a UFCA.

Seção V

Da Gestão de Operações e Comunicações

Art. 14 As operações de TI e as redes de comunicação devem ser gerenciadas de forma segura, abrangendo a proteção contra códigos maliciosos, a realização de cópias de segurança (*backup*), a segregação de ambientes (desenvolvimento, teste e produção), o gerenciamento de acesso remoto e o uso seguro de serviços em nuvem.

§ 1º A rede corporativa e seus dispositivos devem ser continuamente monitorados para defesa contra ameaças e prevenção de acessos indevidos.

§ 2º A aquisição e o desenvolvimento de *softwares* devem seguir um ciclo de vida seguro para prevenir, detectar e corrigir vulnerabilidades.

Seção VI

Do Controle de Acesso

Art. 15 O acesso aos ativos de informação deve ser controlado e limitado com base no princípio do menor privilégio, garantindo que usuários, processos e sistemas acessem apenas os recursos estritamente necessários para o desempenho de suas funções.

Seção VII

Da Gestão de Riscos

Art. 16 A gestão de riscos de segurança da informação tem por objetivo identificar, analisar, avaliar e tratar os riscos, a fim de mantê-los em níveis aceitáveis para a UFCA.

Parágrafo único. A metodologia de gestão de riscos deve estar alinhada ao modelo de gestão de riscos institucional e contemplar critérios de avaliação e aceitação de riscos, resultando em um plano e relatórios de tratamento que serão revisados periodicamente.

Seção VIII

Da Gestão de Continuidade

Art. 17 A gestão de continuidade de negócios visa garantir a resiliência operacional da UFCA e a capacidade de recuperar suas atividades e ativos de informação em tempo hábil após a ocorrência de um desastre ou incidente disruptivo.

Seção IX

Da Gestão de Mudanças

Art. 18 A gestão de mudanças nos aspectos relativos à segurança da informação tem por objetivo preparar e adaptar a UFCA para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências.

Parágrafo único. O processo de gestão de mudanças visa garantir que todas as alterações sejam avaliadas, aprovadas, testadas e implementadas de maneira a minimizar riscos, interrupções não planejadas e vulnerabilidades de segurança.

Seção X

Da Gestão de Vulnerabilidades

Art. 19 A UFCA deve manter um processo contínuo para identificar, avaliar, tratar e monitorar vulnerabilidades técnicas em seus sistemas, ambientes e ativos de informação.

Parágrafo único. O processo de gestão de vulnerabilidades deve incluir, no mínimo:

I - realização de varreduras e análises técnicas periódicas;

II - execução de testes de invasão (pentests); e

III - ações de remediação e mitigação para corrigir as vulnerabilidades identificadas em tempo hábil.

Seção XI

Da Gestão de Fornecedores e Terceiros

Art. 20 A segurança da informação deve ser mantida em todos os acordos com fornecedores e terceiros que tenham acesso, processem ou gerenciem informações e ativos da UFCA.

Parágrafo único. Editais, contratos e acordos devem conter cláusulas que exijam o cumprimento desta POSIN e de suas normas complementares por parte de fornecedores e terceiros.

Seção XII - Da Gestão de Registros de Auditoria (Logs)

Art. 21 Registros de auditoria (logs) relevantes para a segurança devem ser gerados, armazenados de forma segura e retidos por um período definido conforme recomenda a legislação pertinente, a fim de permitir o monitoramento, a análise e a investigação de incidentes.

Seção XIII

Da Auditoria e Conformidade

Art. 22 A UFCA deve realizar auditorias periódicas, internas ou externas, para verificar a conformidade de seus processos, sistemas e controles com esta POSIN, suas normas complementares e a legislação vigente.

Parágrafo único. Os resultados das auditorias devem ser reportados à Alta Administração. As não conformidades identificadas devem ser tratadas por meio de planos de ação corretiva.

Seção XIV

Da Conscientização, Educação e Treinamento

Art. 23 Um programa contínuo de conscientização, educação e treinamento em segurança da informação deve ser mantido e destinado a todos os usuários, com o objetivo de promover uma cultura de segurança e mitigar riscos de origem humana.

Parágrafo único. Esta POSIN e suas normas complementares devem ser amplamente divulgadas, de forma clara e acessível, a todos os colaboradores da UFCA.

CAPÍTULO VII

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Art. 24 A segurança da informação é responsabilidade de todos os usuários dos recursos e serviços de TI. Para isso, é essencial adotar hábitos, posturas e cuidados que garantam a proteção e a privacidade dos dados.

Seção I

Da Alta Administração

Art. 25 Compete à alta administração as seguintes responsabilidades:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional, leis e regulamentos pertinentes;

II - garantir os recursos (humanos, tecnológicos e financeiros) necessários para ações relacionadas à execução da Política de Segurança da Informação no âmbito da UFCA;

III - aprovar os processos de segurança da informação;

IV - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

V - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VI - designar pelo menos um servidor efetivo lotado na UFCA, como responsável pela avaliação de conformidade de acordo com os aspectos relativos à segurança da informação;

VII - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

VIII - aplicar as ações corretivas e administrativas cabíveis, nos casos de violação da segurança da informação; e

IX - aprovar e divulgar a Política de Segurança da Informação da UFCA, bem como suas alterações e atualizações.

Seção II

Do Gestor de Tecnologia da Informação

Art. 26 Compete ao Gestor de Tecnologia da Informação as seguintes responsabilidades:

I - planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

Seção III

Do Gestor de Segurança da Informação

Art. 27 Compete ao Gestor de Segurança da Informação as seguintes responsabilidades:

I - coordenar a elaboração da Política de Segurança da Informação e das normas internas complementares de segurança da informação da UFCA, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República ou órgão equivalente e as melhores práticas sobre o assunto;

II - assessorar a alta administração na implementação da Política de Segurança da Informação;

III - coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos da UFCA;

IV - coordenar a gestão de riscos de segurança da informação, bem como designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos da UFCA;

V - aprovar o plano de gestão de riscos de segurança da informação e os relatórios de identificação, análise, avaliação e tratamento de riscos;

VI - coordenar o processo de gestão de continuidade de negócios em segurança da informação, bem como designar um agente responsável pela referida gestão, dentre os servidores efetivos da UFCA;

VII - coordenar a gestão de mudanças no que se refere à segurança da informação, bem como designar o agente responsável pela gestão de mudança relacionada a segurança da informação, dentre os servidores efetivos da UFCA;

VIII - proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação;

IX - fornecer, ao(s) agente(s) responsável(is) pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação;

X - emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação;

XI - adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração;

XII - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

XIII - promover, com apoio da alta administração, a ampla divulgação da POSIN, das normas internas complementares de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os usuários, a fim de que esses tomem conhecimento de tais instrumentos;

XIV - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

XV - propor recursos e medidas necessárias à execução de ações de segurança da informação;

XVI - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XVII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

XVIII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XIX - fomentar e coordenar ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores; e

XX - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República ou órgão equivalente em assuntos relativos à segurança da informação.

Seção IV

Do Comitê de Governança da UFCA

Art. 28 Compete ao Comitê de Governança da UFCA as seguintes responsabilidades:

I - assessorar na implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Política de Segurança da Informação e das normas internas complementares de segurança da informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas complementares de segurança da informação;

V - deliberar sobre normas internas de segurança da informação; e

VI - avaliar as ações propostas pelo gestor de segurança da informação.

Seção V

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

Art. 29 Compete à ETIR:

I – Monitorar e registrar atividades suspeitas ou incidentes nas redes de dados;

II – Diagnosticar e classificar incidentes de segurança, definindo suas causas e impactos;

III – Executar ações de contenção, erradicação e recuperação para mitigar os danos de incidentes de segurança;

IV – Elaborar relatórios técnicos sobre os incidentes tratados e suas respectivas resoluções;

V – Desenvolver e manter atualizado o plano de resposta a incidentes de segurança;

VI – Identificar, registrar, analisar e mitigar incidentes de segurança relacionados às redes de dados e sistemas computacionais da UFCA;

VII – Implementar ações preventivas e corretivas para a melhoria contínua da segurança da informação;

VIII – Propor normas, políticas e procedimentos que garantam a integridade, confidencialidade e disponibilidade dos dados institucionais;

IX – Promover ações de conscientização e capacitação para a comunidade acadêmica e administrativa sobre boas práticas de segurança digital;

X – Atuar em articulação com outras instituições, quando necessário, para garantir a resposta coordenada a incidentes de segurança cibernética.

Seção VI

Da Unidade de Controle Interno

Art. 30 Compete à Unidade de Controle Interno a seguinte responsabilidade:

I - atuar no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa de segurança da informação conforme legislação pertinente.

Seção VII

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 31 Compete ao Encarregado de Tratamento de Dados as seguintes responsabilidades:

I - conduzir o diagnóstico de privacidade de dados pessoais; e

II - orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, nos termos da legislação vigente no âmbito da administração pública federal.

Seção VIII

Dos Usuários

Art. 32 Compete aos usuários:

I - conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da UFCA;

II - adotar boas práticas de proteção de dados e segurança da informação;

III - comunicar ao UFCA sempre que tomar ciência de evento adverso que possa configurar incidente de segurança da informação;

IV - colaborar com as investigações de incidentes de segurança da informação; e

V - propor melhorias à segurança da informação no âmbito da UFCA.

CAPÍTULO VIII

DAS PENALIDADES

Art. 33 Ações que violem esta Política de Segurança da Informação ou quaisquer de suas diretrizes, normas complementares, procedimentos ou controles de segurança da informação podem ser objeto de investigação e sujeitar-se a sanções administrativas, civis ou penais, conforme o caso.

§ 1º É vedada qualquer ação que não esteja explicitamente permitida na POSIN da UFCA ou que não tenha sido previamente autorizada pelo Comitê de Governança.

§ 2º Casos omissos não tratados nesta POSIN serão submetidos, analisados, tratados e decididos pelo Comitê de Governança.

CAPÍTULO IX
DA POLÍTICA DE ATUALIZAÇÃO

Art. 34 Esta POSIN bem como as políticas e normas internas complementares geradas a partir dela devem ser revisadas, aprovadas e atualizadas em função de alterações nas normativas da UFCA, legislação pertinente, diretrizes e políticas do governo federal ou quando considerada necessária pelo Comitê de Segurança da Informação, não devendo exceder 4 (quatro) anos, conforme Instrução Normativa nº 1, de 27 de maio de 2020.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 35 Esta POSIN e suas atualizações, bem como políticas e normas internas complementares específicas de segurança da informação da UFCA, devem ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 36 Esta política entra em vigor a partir da data de sua publicação.

SILVÉRIO DE PAIVA FREITAS JR.

Reitor

Presidente do Comitê de Governança