Boletim de Serviço Eletrônico em 01/07/2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARA

RESOLUÇÃO Nº 04/CATI, DE 15 DE ABRIL DE 2025

Institui a nova versão da Política de Segurança da Informação (POSIC) da Universidade Federal do Ceará.

O REITOR DA UNIVERSIDADE FEDERAL DO CEARÁ, CEARÁ, no uso de suas atribuições legais e estatutárias, e em atendimento à recomendação expressa do Comitê Administrativo de Tecnologia da Informação e Governança Digital (CATI), em sua reunião de 15 de abril de 2025,

CONSIDERANDO o recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visando a auxiliar o atendimento previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD),

RESOLVE:

Art. 1º Aprovar a revisão da Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal do Ceará (UFC).

Art. 2º Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

CUSTÓDIO LUÍS SILVA DE ALMEIDA
Reitor

COMITÊ ADMINISTRATIVO DE TECNOLOGIA DA INFORMAÇÃO E GOVERNANÇA DIGITAL
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC) DA UNIVERSIDADE FEDERAL DO CEARÁ

Histórico de versões

Data	Versão	Descrição	Autor
19/07/2011	1.0	Produção da versão inicial	Márcio Correia
10/11/2011	1.1	Realizados ajustes aprovados na reunião com os Diretores Geral e Adjunto da STI. Correções ortográficas. Ajustes nos conceitos e definições utilizados. Realizadas também melhorias no detalhamento e adequação das Competências e Responsabilidades.	Márcio Correia
31/05/2012	2.0	Realizados ajustes aprovados em 27/04/2012 na reunião do CATI. Ajustes de alguns princípios, definições e termos utilizados. O item “3. Princípios” foi reescrito com foco na	Márcio Correia

Data	Versão	Descrição	Autor
		comunicação com o usuário e perdeu o caráter regulatório. Foi removido o item “4.1 b” que tratava da propriedade das informações produzidas na instituição	
05/06/2013	2.1	Realizados ajustes aprovados em 05/06/2013 na reunião do CATI. Atendendo sugestões da Auditoria Interna, enviados à STI via Solicitação de Auditoria no 022/2012.	Márcio Correia
15/03/2021	3.0	Realizados ajustes pela adequação a nova estrutura da Superintendência de Tecnologia da Informação com a criação da Coordenadoria de Infraestrutura e Segurança da Informação (CISI)	Coordenadoria de Infraestrutura e Segurança da Informação (CISI)
24/03/2025	4.0	Adequação ao modelo do Programa de Privacidade e Segurança da Informação – PPSI do Ministério da Gestão e Inovação em serviço Público (MGI)	Coordenadoria de Infraestrutura e Segurança da Informação (CISI)

Sumário

INTRODUÇÃO

Cada vez mais o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo, enquanto agente de tratamento, está designada no art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018:

> “Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”

Essa proteção é contra vários tipos de ameaças que, se efetivadas, podem gerar prejuízos à organização. A Segurança das Informações pode ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e soluções de Tecnologia da Informação (TI).

PROPÓSITO

A Segurança da Informação, ou simplesmente SI, é a proteção da informação nas suas mais diversas formas. Não importa se ela é escrita, impressa ou armazenada digitalmente. Nem se ela é transmitida pelo correio ou por e-mail. Essa proteção é contra vários tipos de ameaças que, se efetivadas, podem gerar prejuízos à organização.

Segurança da Informação é fundamental para os negócios, inclusive do setor público. Nesse caso, a Segurança da Informação assume papel importante nos serviços de governo eletrônico (e-gov), ao evitar ou reduzir os riscos de fraude, sabotagem, vandalismo, incêndios e inundações, além de proteger as infraestruturas críticas das organizações.

Esta política estabelece regras, diretrizes e práticas para a segurança da informação dentro da Universidade Federal do Ceará (UFC). Visa a garantir a confidencialidade, integridade e disponibilidade da informação, assegurando seu uso adequado e a mitigação de riscos à segurança da informação. Estipular papéis e responsabilidades claras e objetivas, definir diretrizes de segurança e estabelecer meios de monitoramento do cumprimento desta política, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

A Política de Segurança da Informação e Comunicação é um documento que contém um conjunto de princípios e diretrizes que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da organização, bem como por seus usuários internos e externos, a fim de garantir que os Ativos sejam assegurados.

ESCOPO

Instituir a Política de Segurança da Informação (PSI), no âmbito da Universidade Federal do Ceará (UFC), com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política se aplica a todos os ativos de informação da Universidade Federal do Ceará (UFC), incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela Universidade Federal do Ceará (UFC) e entidades subsidiárias.

Apresentar de forma clara a visão desta instituição, e de sua administração superior, relacionada à Segurança da Informação e Privacidade. Definir diretrizes que orientarão a criação de normas e procedimentos relacionados à segurança da informação e privacidade no âmbito desta instituição, provendo meios para atingir a excelência na qualidade dos serviços prestados por esta instituição, no que tange à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações.

TERMOS E DEFINIÇÕES

Para efeito desta política, serão adotadas as seguintes definições:

ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. Administração Pública Federal (APF). Responsável pelo atendimento aos incidentes em redes de computadores da APF;

AGENTE RESPONSÁVEL: é o servidor designado no documento de criação da ETIR e responsável pela mesma, é também o ponto de contato entre a ETIR e o CTIR Gov;

ARTEFATO MALICIOSO: qualquer programa de computador, ou parte dele, construído com a intenção de causar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

ATIVO CUSTODIADO: ativo de terceiro que é administrado e conservado por esta instituição;

ATIVO DE INFORMAÇÃO: ativo que guarda informação de valor para esta instituição;

CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

CONFORMIDADE EM SI: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização;

CTIR Gov: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo Federal.

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

DIRETRIZ: conjunto de orientações que devem ser observadas para a produção de Normas e Procedimentos específicos;

DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

E-MAIL INSTITUCIONAL: serviço de correio eletrônico oferecido por esta instituição para seus servidores como instrumento de trabalho.

EVENTO: qualquer ocorrência observável em um sistema ou rede de computadores;

INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou redes de computadores. Nesse documento o termo “incidente” será utilizado com o mesmo significado de “incidente de segurança” aqui definido;

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

MEMBROS: todo corpo docente, discente, técnico-administrativo e prestadores de serviços;

NORMA: conjunto de regras que devem ser seguidas por um grupo;

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da instituição, bem como por seus usuários internos e externos, a fim de garantir que os Ativos sejam assegurados;

SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

SERVIÇOS (ETIR): é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido ao público-alvo da ETIR;

Spam: termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES DE COMPUTADORES: conjunto de ações que visam receber, analisar e responder os incidentes de segurança ocorridos em uma rede e/ou sistema computacional;

VULNERABILIDADE: qualquer fragilidade dos sistemas e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação (POSIC) da Universidade Federal do Ceará (UFC), com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da Segurança da Informação (SI).

Art. 2º Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais da Universidade Federal do Ceará (UFC), e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade desta Instituição.

Seção I
Do Objetivo

Art. 3º São objetivos da Política de Segurança da Informação:

§ 1º estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

§ 2º estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

§ 3º estabelecer competências e responsabilidades quanto à segurança da informação;

§ 4º nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação; e promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da Universidade Federal do Ceará (UFC).

Art. 4º Para os efeitos desta Política e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO II
DOS PRINCÍPIOS E DIRETRIZES

Art. 5º As ações de segurança da informação da Universidade Federal do Ceará são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais para o funcionamento da Universidade Federal do Ceará;

III - economicidade da proteção dos ativos de informação;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V - observância da publicidade como preceito geral e do sigilo como exceção;

VI - responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII - alinhamento estratégico da Política de Segurança da Informação e Comunicação com o planejamento estratégico da Universidade Federal do Ceará, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VIII - conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

IX - educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito da Universidade Federal do Ceará e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º As normas, procedimentos, manuais e metodologias de segurança da informação da da Universidade Federal do Ceará devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º As ações de segurança da informação devem:

§ 1º considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da Universidade Federal do Ceará;

§ 2º ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da Universidade Federal do Ceará;

§ 3º Ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e visar à prevenção da ocorrência de incidentes.

Art. 9º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos a Universidade Federal do Ceará.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na Universidade Federal do Ceará compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor. Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional da Universidade Federal do Ceará, são passíveis de monitoramento e auditoria, respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do(a) da Universidade Federal do Ceará a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da Universidade Federal do Ceará.

Art. 12. A Política de Segurança da Informação e Comunicação e suas atualizações, bem como normas específicas de segurança da informação da Universidade Federal do Ceará, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 13. Todos os contratos de prestação de serviços firmados pela Universidade Federal do Ceará conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como suas normas decorrentes.

CAPÍTULO III
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 14. A estrutura de Gestão de Segurança da Informação é composta por:

I - Alta Administração;

II - Comitê de Segurança da Informação;

III - Gestor de Segurança da Informação;

IV - Gestor de Tecnologia da Informação e Comunicação;

V - Encarregado pelo Tratamento de Dados Pessoais;

VI - Responsável pela Unidade de Controle Interno; VII - Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VIII - Usuários de Informação.

Art. 15. Compete à Alta Administração:

§ 1º fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da Universidade Federal do Ceará, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

§ 2º formalizar e aprovar a Política de Segurança da Informação e Comunicação da Universidade Federal do Ceará, através do Comitê Administrativo de Tecnologia da Informação e Governança Digital (CATI), bem como suas alterações e atualizações.

Art. 16. Compete ao Comitê de Segurança da Informação:

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 de segurança da informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas 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.

§ 1º A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação será definido em Portaria emitida pela Superintendência de Tecnologia da Informação (STI), de acordo com a legislação vigente.

§ 2º O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

Art. 17. Compete ao Gestor de Segurança da Informação:

I - coordenar o Comitê de Segurança da Informação;

II - coordenar a elaboração da Política de Segurança da Informação e Comunicação - POSIC e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III - assessorar a Alta Administração na implementação da Política de Segurança da Informação e Comunicação;

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

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no

órgão;

VI - incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

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

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

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

XI - manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

Parágrafo único. O Gestor de Segurança da Informação da Universidade Federal do Ceará será designado em Portaria, de acordo com a legislação vigente.

Art. 18. Compete ao Gestor de Tecnologia da Informação e Comunicação, de acordo com o disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 19. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, de acordo com o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como 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.

Art. 20. Compete ao Responsável pela Unidade de Controle Interno apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 21. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na Universidade Federal do Ceará;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação; e

VII - promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em Portaria emitida pela Superintendência de Tecnologia da Informação (STI), de acordo com a legislação vigente.

Art. 22. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da Universidade Federal do Ceará. Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 23. A Política de Segurança da Informação e Comunicação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 24. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes em segurança da informação;

IV - gestão de ativos;

V - gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI - controles de acesso;

VII - gestão de riscos;

VIII - gestão de continuidade de negócios; e

IX - auditoria e conformidade;

Parágrafo Único. Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 25. As políticas, normas, procedimentos, orientações ou manuais de que trata o §2º do art. 16 devem abordar, no mínimo, aspectos relacionados:

I - a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de dados (ANPD);

II - a classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III - a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV - ao uso aceitável da informação e a utilização de mídias de armazenamento;

V - a entrada e saída de ativos de informação das instalações da organização;

VI - aos perímetros de segurança da organização;

VII - aos controles de acesso baseados no princípio do menor privilégio;

VIII - as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;

IX - aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;

X - ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

XI - a Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização; a manutenção de inventario atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XII - a utilização adequada dos recursos operacionais e de comunicações fornecidos pela Universidade Federal do Ceará, a serem utilizados para fins profissionais, relacionados às atividades da Instituição, em conformidade com os princípios éticos e profissionais, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação da UFC;

XIII - aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV - o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV - o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XVI - as políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII - as políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação da Universidade Federal do Ceará;

XVIII - as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente da UFC, dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIX - as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que a Universidade Federal do Ceará possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX - as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças; e

XXI - as políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

§ 1º As unidades organizacionais da Universidade Federal do Ceará devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades da Universidade Federal do Ceará, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos na Universidade Federal do Ceará devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes

CAPÍTULO IV
DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 26. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo Universidade Federal do Ceará para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 27. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela Universidade Federal do Ceará.

Art. 28. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 29. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 30. As unidades organizacionais da Universidade Federal do Ceará devem permitir e incentivar a participação em ações de treinamento e conscientização para que os seus servidores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Art. 31. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através de processo SEI encaminhado a Coordenadoria de Infraestrutura e Segurança da Informação (CISI) da Superintendência de Tecnologia da Informação (STI).

Art. 32. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela UFC periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 33. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 34. Esta Política será revisada, pelo menos a cada quatro anos, para refletir as mudanças nos riscos à segurança da informação, nas melhores práticas e no ambiente da Universidade Federal do Ceará.

Art. 35. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e Comunicação e seus documentos devem ser submetidos ao Comitê de Segurança da Informação via processo SEI encaminhado à Coordenadoria de Infraestrutura e Segurança da Informação (CISI) da Superintendência de Tecnologia da Informação (STI).

Art. 36. É proibida a utilização do E-mail Institucional para fins que não caracterizem ou prestem suporte às atividades de pesquisa, ensino e extensão.

Art. 37. Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

§ 1º Não devem ser solicitadas informações pessoais dos usuários através de correio eletrônico.

§ 2º O usuário não deve clicar em links que solicitem a atualização de suas informações pessoais.

§ 3º O usuário deve reportar à Coordenadoria de Infraestrutura e Segurança da Informação sobre o recebimento de mensagens suspeitas ou que viole esta norma.

§ 4º É proibido o envio de grande quantidade de mensagens do tipo spam, ficando o responsável pelo envio das mensagens sujeitos à penalidade prevista nesta norma.

§ 5º O usuário tem total responsabilidade pelo envio de anexos nas mensagens, ficando o mesmo também responsável pela garantia da não violação do princípio da legalidade.

Art. 38 Das normas para uso da internet.

§ 1º É proibido o acesso a sítios com conteúdo indevido ou inadequado ao ambiente de trabalho.

§ 2º Em caso de necessidade de acesso a um sítio que esteja bloqueado, a solicitação de liberação deve ser feita formalmente à STI. Embora um site com conteúdo ilegal não esteja bloqueado, não implica dizer que o acesso ao mesmo seja permitido.

§ 3º Todos os usuários devem utilizar o acesso à internet respeitando o código de ética desta universidade.

§ 4º É proibida a utilização de software P2P (tais como µTorrent, BitTorrent, Emule e similares). Em casos excepcionais a solicitação de liberação deve ser feita formalmente à STI.

§ 5º É proibida a realização de download de software que infringe os direitos autorais.

§ 6º É proibida a utilização de serviços de anonimato para acesso à internet.

§ 7º Todos os servidores, terceirizados contratados e outros agentes que utilizam os recursos de rede são responsáveis pela segurança, zelo e bom uso das informações às quais têm acesso, sejam elas do próprio governo, do cidadão ou de outro órgão.

§ 8º Todos os sítios e sistemas que lidam com dados sensíveis devem implementar protocolo criptográfico forte.

§ 9º Nas configurações das redes sem fio da UFC deverá ser utilizado um sistema de autenticação de usuários para o acesso ao serviço, utilizar um protocolo criptográfico forte para o tráfego dos dados da rede sem fio e ser utilizado um sistema que gerencie os pontos de acessos.

§10. É de responsabilidade da UFC promover a filtragem de acessos indevidos provenientes de suas redes, com destino a outra(s) rede(s) de outros órgãos, ou para a Internet, que podem ser gerados por ataques direcionados, códigos maliciosos (malware) e ataques de negação de serviço (DDoS), dentre outros.

Art. 39 Esta política entra em vigor na data de sua aprovação.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação— Requisitos. Rio de Janeiro, 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 jul. 2024.

BRASIL. Presidência da República. Casa Civil. Instituto Nacional de Tecnologia da Informação. Portaria N° 79, de 31 de dezembro de 2018. Política de Segurança da Informação e

Comunicações do Instituto Nacional de Tecnologia da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 02 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Decreto/D9637.html. Acesso em: 17 jun. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-%202 19115663. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/ptbr/composicao/SSIC/dsic/legislacao/copy_of_IN01_consolid ada.pdf. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 03, de 28 de maio de 2021. Brasília, DF, GSI/PR, 2021. Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN03_consolidada.pdf. Acesso em: 01 jul. 2024.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. Guia do Framework de Privacidade e Segurança da Informação. Março 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framewo rk_psi.pdf . Acesso em: 25 jun. 2024.

BRASIL. Presidência da República. Agência Nacional de Proteção de Dados - ANPD. Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicaco es/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 01 jul. 2022.

Documento assinado eletronicamente por **CUSTODIO LUIS SILVA DE ALMEIDA**, **Reitor**, em 01/07/2025, às 11:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5711388** e o código CRC **727DC408**.