RESOLUÇÃO Nº 1879/2023 – CONSU, 30 de junho de 2023.

DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DA UNIVERSIDADE ESTADUAL DO CEARÁ.

O Reitor da Universidade Estadual do Ceará – UECE, no uso de suas atribuições estatutárias e regimentais, considerando o que consta do Processo SUITE Nº 31032.000310/2023-85 e a deliberação dos Conselheiros presentes à sessão do Conselho Universitário – CONSU, realizada no dia 30 de junho de 2023,

CONSIDERANDO as orientações definidas no Decreto Nº 34.100 de 8 de junho de 2021 (Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e Comunicação - TIC do Governo do Estado do Ceará e sobre o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará - CGSI);

CONSIDERANDO a Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014);

CONSIDERANDO a importância do estabelecimento de normas e procedimentos de forma a garantir a integridade, confidencialidade e disponibilidade das informações no contexto da FUNECE,

RESOLVE:

Art. 1º. Regulamentar a política de segurança da informação e comunicação no âmbito do Sistema FUNECE/UECE, estabelecendo as diretrizes básicas a serem seguidas pelos usuários e administradores do serviço.

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

Parágrafo único. Fica revogada a Resolução a Nº. 390/2002 - CONSU.

Reitoria da Universidade Estadual do Ceará – UECE, Fortaleza, 30 de junho de 2023.

HIDELBRANDO DOS SANTOS SOARES:50082345368
Assinado de forma digital por HIDELBRANDO DOS SANTOS SOARES:50082345368
Dados: 2023.07.12 14:34:29 -03'00'

Prof. M.e. Hidelbrando dos Santos Soares
Reitor da UECE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DA UNIVERSIDADE ESTADUAL DO CEARÁ

CAPÍTULO I
DOS CONCEITOS E DAS DEFINIÇÕES

Art. 1º. Entende-se por conceitos, definições e termos utilizados nesta política:

I. Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na UECE;
II. Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;
III. Ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
IV. Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
V. Ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
VI. Usuário: servidores, docentes, discentes e colaboradores que usufruem dos sites e sistemas corporativos de TIC do sistema FUNECE/UECE;
VIII. Comunicação: no contexto da Política de Segurança da Informação e Comunicação, comunicação se refere a transmissão de dados;
XI. Serviço de rede: processo de software que estabelece conexões de rede para fornecer armazenamento, manipulação, apresentação e/ou transmissão de dados ou outra capacidade;
XII. Usuário da informação: todos que tenham acesso a ativo físico, de informação e de software;
XIII. Incidente de segurança: qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de Segurança da Informação; (texto aprovado em reunião);
XIV. Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pelo Comitê de Segurança da Informação e Comunicações, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
XV. Logs: registros de atividades dos usuários efetuadas nos domínios uece.br;
XVI. Incidente de segurança: qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de segurança da informação; (texto aprovado em reunião)
XVII. Ambiente de produção: termo usado para descrever a configuração em que software e outros produtos são colocados efetivamente em operação para os usos pretendidos pelos usuários finais;
XVIII. Ambiente de homologação ou teste: é utilizado pela equipe de desenvolvimento e descreve a configuração utilizada durante o processo de desenvolvimento ou atualização dos sistemas de software e outros produtos são colocados efetivamente em operação para os usos pretendidos pelos usuários finais.

CAPÍTULO II
DISPOSIÇÕES PRELIMINARES

Art. 2º. A Política de Segurança da Informação e Comunicação (POSIC) da Universidade Estadual do Ceará (UECE) visa estabelecer diretrizes estratégicas, responsabilidades e competências para o manuseio da informação da instituição ou sob sua responsabilidade, de forma eletrônica ou não, observando os requisitos mínimos de confidencialidade, integridade, disponibilidade e autenticidade, além do atendimento à legislação pertinente, e normas definidas pelos órgãos reguladores.

§1º. A POSIC é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda.

§2º. As diretrizes estabelecidas nesta política devem estar alinhadas ao Estatuto Regimento Geral da UECE, e em consonância com os valores institucionais e demais disposições vigentes.

§3º. Essa política se aplica a todos os usuários no que diz respeito a seus direitos e responsabilidades com os recursos computacionais da instituição e as informações neles armazenados, e se aplica a todas as unidades administrativas, servidores, estudantes, prestadores de serviço autorizados, e usuários de serviços de TIC e dos sistemas de informação mantidos na UECE.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 3º. O compromisso da UECE com o tratamento adequado de suas informações, assim como as de seus usuários, está fundamentado nos seguintes princípios:

I. 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;
II. Integridade: propriedade que garante que a informação não seja modificada ou destruída de maneira não autorizada ou acidental;
III. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
IV. Autenticidade: propriedade que consiste na segurança de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade, ou seja, relaciona-se com a confirmação de autoria, a certificação e a originalidade da informação;
V. Não repudiação: propriedade pela qual se previne que uma entidade (emissor ou receptor) negue a participação em uma troca de informação;
VI. Legalidade: diz respeito à obediência aos princípios constitucionais, administrativos e à legislação vigente.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 4º. A segurança da informação e comunicação deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidades e cuidados constantes no momento do uso dos ativos de informação.

Parágrafo único. A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 5º. É responsabilidade da Administração Superior prover a orientação e o apoio às ações de segurança da informação, de acordo com os objetivos estratégicos e com as leis e os regulamentos pertinentes.

Art. 6º. É responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes estabelecidas nesta política no âmbito de suas áreas de atuação.

Art. 7º. É responsabilidade de todos que têm acesso aos ativos de informação da UECE manter cuidados e níveis adequados de segurança da informação tratada, segundo preceitos desta política e de suas normas complementares.

Art. 8º. É responsabilidade de todos que têm acesso aos ativos de informação da UECE comunicar de forma imediata ao DETIC (atendimentodi@uece.br) a ocorrência de incidentes que possam afetar a segurança dos mesmos.

Art. 9º. É responsabilidade do DETIC a gestão dos sistemas de informação e dos recursos computacionais de processamento e transmissão de dados da UECE.

§1º. É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir esta política de segurança, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes

§2º. É vedada a instalação de recursos de infraestrutura de rede no parque computacional da Universidade sem autorização do DETIC.

§3º. É vedada a desinstalação ou alteração das configurações (lógica ou física) de recursos computacionais e de rede no parque computacional da universidade sem autorização do DETIC.

CAPÍTULO IV
DOS ATIVOS DE INFORMAÇÃO

Art. 10. É de responsabilidade dos dirigentes de setor/departamento a classificação das informações manuseadas em seu setor, observando a legislação e regulamentações pertinentes, considerando também os critérios de sigilo, valor e criticidade.

§1º. Os servidores e demais colaboradores de cada setor devem ser orientados sobre a classificação das informações a que têm acesso, bem como os cuidados necessários no tratamento delas.

§2º. Os ativos de informação devem ser classificados em níveis de criticidade, considerando o provável impacto no caso de quebra de segurança.

§3º. Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.

Art. 11. A gestão dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Parágrafo único. O tratamento de dados pessoais deverá observar resolução específica sobre privacidade e tratamento no contexto do sistema FUNECE/UECE.

Art. 12. Os ativos de informação são destinados ao uso corporativo e acadêmico, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

Parágrafo único. O usuário deve ter acesso aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

Art. 13. Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores, dispositivos móveis, dispositivos de armazenamento externo, entre outros) são de sua responsabilidade, cabendo a eles adotar as medidas necessárias para realizar as cópias de segurança desses ativos e proceder à sua recuperação em caso de perda.

Art. 14. Quando da celebração de contratos, estes deverão conter, obrigatoriamente, cláusulas específicas sobre o sigilo, confidencialidade e uso das informações como condição imprescindível para que possa ser concedido o acesso às informações.

CAPÍTULO IV
DOS PROTOCOLOS DE SEGURANÇA

Art. 15. Os processos e as atividades que sustentam os serviços críticos disponibilizados pela UECE devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e das comunicações.

Art. 16. É de responsabilidade do Departamento de Tecnologia da Informação e Comunicação da UECE (DETIC) a definição e realização dos procedimentos relacionados à política de cópia de segurança (*backup*) e recuperação de sistemas e dados armazenados.

Parágrafo único. O prazo para o armazenamento das informações em *backup* deverá atender às regulamentações pertinentes e aos requisitos da área responsável pela utilização desses sistemas.

Art. 17. O DETIC será responsável pelo fornecimento, pela instalação e pela manutenção das soluções para segurança lógica (vírus, *malwares*, acesso não autorizado, invasões etc.) nos computadores, servidores de rede e demais equipamentos que sejam de propriedade da UECE.

§1º. Deverá ser instalado no parque computacional da Universidade (computadores, *notebooks* e demais equipamentos conectados à rede de dados da UECE), sempre que possível, *softwares* para prevenção de código malicioso.

§2º. Os usuários devem ser orientados a utilizar o *software* para prevenção de código malicioso para verificar unidades externas de armazenamento de arquivos antes de sua utilização. Também devem ser verificados os arquivos recebidos por e-mail e outras modalidades de transferência de arquivos.

Art. 18. A gestão de incidentes de segurança da informação prevê a identificação dos mesmos, monitoramento e tratamento, de forma a garantir a continuidade das atividades e minimizando seus impactos, assim como por eventuais notificações por parte das entidades competentes.

Art. 19. Para os sistemas de missão crítica, deverão ser contratados serviços ou utilizados equipamentos que disponham de recursos de redundância de processamento e de armazenamento de dados.

Art. 20. Os servidores computacionais, onde se encontram os sistemas de missão crítica, devem estar em sala segura contra problemas de segurança física (instabilidade elétrica, condições ambientais adversas (temperatura, umidade, desastres naturais, incêndios, acesso indevido etc).

CAPÍTULO VI
DO CONTROLE DE ACESSO

Art. 21. Todo ambiente deve ser classificado e protegido com mecanismos adequados de segurança de acordo com a criticidade e o sigilo dos ativos que são mantidos naquele local.

Art. 22. Cabe ao DETIC implementar os controles físicos e lógicos necessários para impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações, além de prevenir o acesso físico não autorizado, danos e interferências nas informações e em seus recursos de processamento da organização.

Art. 23. O acesso aos recursos da rede e sistemas corporativos da UECE é restringido a pessoas autorizadas, sendo seu uso controlado e **limitado ao mínimo necessário** para o cumprimento das atividades de gestão, ensino, pesquisa ou extensão, no contexto da UECE, previamente autorizada pelo respectivo gestor do ativo.

Parágrafo único. A conta de acesso e a senha de usuário são únicas, individuais e intransferíveis, e representam nível de delegação concedida para o desempenho de suas funções.

Art. 24. Discentes, servidores técnico-administrativos, colaboradores terceirizados e demais colaboradores eventuais terão seu acesso autenticado utilizando login e senha da conta de e-mail institucional concedido de acordo com resolução específica.

Parágrafo único. A desativação da conta de e-mail implicará a inativação dos privilégios de acesso associados ao respectivo e-mail.

Art. 25. Sempre que houver a admissão, mudança das atribuições ou desligamento de membros desta instituição, será responsabilidade da chefia imediata notificar aos gestores dos ativos utilizados por esse membro. Os gestores dos ativos deverão providenciar os ajustes necessários dos privilégios de acesso dos respectivos ativos.

Art. 26. Em caso de usuário visitante, poderá ser feito o cadastro de conta de acesso para este desde que solicitado pelo responsável do setor onde realizará suas atividades, estabelecendo um prazo de validade para a conta criada.

Art. 27. A conta de acesso do usuário poderá ser bloqueada, em caso de incidentes de segurança da informação e comunicações causados por este. A conta será restabelecida após a solução dos problemas causados desde que não existam outros impedimentos.

Art. 28. É de responsabilidade do DETIC monitorar o acesso à rede e aos sistemas para identificar problemas relativos à segurança da informação.

Parágrafo único. Os registros de auditoria (logs) devem conter as informações de monitoramento por tempo acordado para atender às regulamentações pertinentes e servir de auxílio em caso de investigações pelas autoridades competentes.

CAPÍTULO VII
DA SEGREGAÇÃO DE AMBIENTES

Art. 29. O DETIC deve assegurar que todos os sistemas de informação, sob sua responsabilidade sejam aderentes às diretrizes a seguir:

I. Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais;
II. Os ambientes de produção somente poderão ser acessados por usuários internos responsáveis pela implantação dos sistemas de informação;
III. O acesso às bases de dados dos ambientes de produção será feito, sempre que possível, por meio dos sistemas de informação ou, não sendo possível, o acesso deverá ser feito por um membro da equipe responsável pela base de dados com autorização de um usuário interno com nível gerencial da área solicitante. O acesso direto deverá ser registrado em meio que permita a identificação do que foi modificado e quem foi responsável pela modificação;
IV. Os sistemas de informação que forem transferidos para o ambiente de produção deverão ter seu código-fonte original mantido por um sistema de gerenciamento de repositórios de código-fonte interno;
V. O código-fonte dos sistemas de informação sob domínio do DETIC deverão ser gerenciados por ferramenta específica de controle de versão que possibilite auditoria. O controle de versão deve permitir a identificação do responsável pela inclusão/exclusão/alteração do código-fonte, assim como a recuperação de versões recentes;
VI. O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não deve ser utilizado para testes. Os testes devem ser feitos em ambiente apropriado e gerenciado;
VII. A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução.

CAPÍTULO VII
DO USO E DAS PENALIDADES PELO USO INDEVIDO

Art. 30. Ao público-alvo não é dado o direito de desconhecimento desta política, devendo este seguir rigorosamente o estabelecido nas normas de segurança.

Art. 31. O descumprimento ou a violação, pelo usuário, das regras previstas nesta resolução e na legislação pertinente a matéria, infringindo suas disposições, estarão sujeitos a processos administrativos, criminais e cíveis.

§1º. No caso de constatação de uso irregular dos serviços, o usuário terá seu acesso bloqueado de forma imediata para averiguação.

§2º. Constatada a irregularidade, será notificada a ocorrência de transgressão ao seu chefe imediato e à diretoria correspondente.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 32. Solicitações de auditorias e de averiguações decorrentes de denúncias ou processos disciplinares que trata o art. 31, deverão ser encaminhados à Presidência da FUNECE, que colocará para apreciação do Conselho Superior Universitário - CONSU.

Art. 33. Esta regulamentação entra em vigor na data de sua publicação.

Parágrafo Único. Os casos omissos serão dirimidos pelo CONSU.