POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação e Comunicação da Universidade Federal de Sergipe (POSIC/UFS) tem como objetivo principal definir as diretrizes para criação de normas e procedimentos que firmam o compromisso da instituição com a proteção e segurança da informação e comunicação no âmbito da universidade, promovendo um serviço de qualidade que preza pela autenticidade, confiabilidade, confidencialidade, disponibilidade, integridade e não-repúdio das informações.

Art. 2º A POSIC está integrada às demais políticas e regimentos da UFS e é fundamentada nas leis vigentes.

Art. 3º As diretrizes e normas estabelecidas nesta política devem ser cumpridas em todo o âmbito da universidade por todos os agentes públicos, colaboradores, terceirizados, parceiros e visitantes que tenham acesso as instalações físicas ou ambientes computacionais e aos ativos de informação pertencentes ou sob custódia da UFS.

Art. 4º As diretrizes e normas estabelecidas nesta política também devem ser aplicadas a todos os ativos de informação incluídos em acordos, parcerias e convênios do gênero estabelecidos entre a UFS e outros órgãos públicos ou privados.

Art. 5º Esta política entra em vigor a partir da data de sua publicação e permanece por tempo indeterminado, enquanto não houver ato normativo que a atualize ou a revogue.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 6º Esta POSIC observará, no que couber, os conceitos do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 26 de setembro de 2019, além dos definidos a seguir:

I. Aspectos da Segurança: a segurança pode ser entendida sob dois aspectos: físico e lógico. A segurança física está relacionada à proteção de edificações, infraestrutura, equipamentos e ativos físicos; a segurança lógica se refere à segurança dos dados em ambiente computacional armazenados nos servidores institucionais e também inclui os dados gerados e armazenados em computadores ou dispositivos utilizados por seus usuários;

II. Ativos TIC: Ativos de Tecnologia de Informação e Comunicação que englobam os ativos de *hardware*, como equipamentos de escritório, de infraestrutura e de multimídia; ativos de *software*, como aplicações desenvolvidas pela UFS, aplicações desenvolvidas por terceiros hospedadas ou administradas pela UFS, aplicações de *software* livre e licenças de aplicações de terceiros adquiridas; e ativos de dados, como dados armazenados em sistemas de informação considerados pessoais ou corporativos;

III. Comitê de Governança Digital (CGD): Comitê responsável pelo desenvolvimento e monitoramento de políticas e diretrizes ligadas à governança digital e segurança da informação na UFS;

IV. Redundância de processamento: Método de duplicação do uso de ferramentas com o intuito de elevar sua confiabilidade e segurança por meio da utilização de meios alternativos em caso de falhas e indisponibilidades;

V. Terceiros e fornecedores: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à Universidade Federal de Sergipe;

VI. Termo de responsabilidade: acordo que visa manter a segurança das informações, atribuindo responsabilidades aos usuários ou ao administrador de serviços, quanto ao sigilo e a correta utilização das informações e dos ativos sob a responsabilidade da UFS;

VII. Usuário: pessoa física habilitada pela UFS para acessar os seus ativos de informação, formalizado ou não por meio da assinatura de Termo de Responsabilidade, seja discente, servidor ou equiparado, empregado ou terceirizado, funcionários ou público externo.

CAPÍTULO III
PRINCÍPIOS E DIRETRIZES GERAIS

Art. 7º A POSIC da UFS visa garantir a preservação das informações necessárias as suas atividades e está fundamentada nos seguintes princípios:

I. Autenticidade: garante a veracidade da autoria da informação;
II. Confidencialidade: somente pessoas devidamente autorizadas devem ter acesso à informação;
III. Integridade: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações;
IV. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário;
V. Legalidade: o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos em vigência;
VI. Transparência das informações de acesso irrestrito;
VII. Proteção das informações com restrição de acesso e dos dados pessoais dos usuários, de acordo com a legislação em vigor.

Art. 8º A segurança da informação é responsabilidade de todos os usuários dos ativos TIC da UFS.

Art. 9º Os dirigentes e chefias das unidades da UFS se comprometem a atuar em colaboração com a STI, adotando e desenvolvendo hábitos e cuidados que visem minimizar vulnerabilidades ou ameaças à universidade.

Art. 10 Os ativos TIC devem ser usados de forma ética, legal e alinhada às finalidades da atividade do usuário.

Art. 11 Normas complementares a essa POSIC e procedimentos sobre a utilização dos serviços de Tecnologia da Informação, bem como termos de uso de tais serviços serão definidos pela STI em documentos específicos e divulgados na página *web* da STI.

Art. 12 A STI deverá propor normas complementares ao Comitê de Segurança da Informação e Comunicações (CSIC), a fim de manter registros, como mecanismo de auditoria que possibilite o rastreamento, acompanhamento, controle e verificação de acesso aos serviços, sistemas de informação e rede interna.

Art. 13 A STI deve propor normas ao CSIC, de forma que os órgãos de TIC possam definir procedimentos e implementar mecanismos de autenticação que determinem a titularidade.

CAPÍTULO IV
DO TRATAMENTO E CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 14 A UFS deve possuir mecanismos para gerir os critérios de acesso, divulgação, bem como o tratamento e classificação da informação, de acordo com a disponibilidade, autenticidade integridade e confidencialidade, quando aplicável, independente do meio de armazenamento e processamento.

Art. 15 O tratamento das informações pessoais dos usuários da UFS deve considerar o respeito à privacidade, bem como às liberdades e garantias individuais.

Art. 16 O compartilhado de dados pessoais dos usuários da UFS será realizado para o cumprimento das suas obrigações legais ou regulatórias com organizações públicas ou privadas, de acordo com a finalidade admitida na legislação vigente, sendo resguardados os princípios de proteção de dados pessoais, cabendo à UFS definir os níveis adequados de segurança dos dados dos seus usuários.

Art. 17 A UFS deverá analisar, avaliar e selecionar todos os documentos físicos e digitais produzidos e acumulados, tendo em vista a identificação daqueles para guarda permanente, bem como para a eliminação dos documentos destituídos de valor de forma autorizada e segura.

Art. 18 As cópias de segurança das informações são responsabilidade de seus responsáveis imediatos.

Art. 19 A STI deverá criar e manter uma Política de Gestão de Ativos que compreenda normas aplicadas a todo o ciclo de vida de recursos TIC no âmbito da universidade.

Art. 20 Todo ativo de dado da UFS deve ser protegido contra códigos maliciosos e qualquer tipo de ataque conforme as regulamentações vigentes, de modo a minimizar riscos ao serviço prestado, às atividades executadas e à imagem institucional.

Art. 21 A UFS deve assegurar que os ativos de dados:

I. Sejam identificados e um inventário com estes ativos seja estruturado, mantido e protegido;
II. Sejam passíveis de monitoramento e auditoria;
III. Tenham o seu ciclo de vida identificado e documentado;
IV. Tenham os seus responsáveis indicados;
V. Tenham a sua entrada e/ou saída das dependências da UFS devidamente registradas e autorizada por gestor competente;
VI. Tenham a sua cessão registrada, quando se tratar de ativos móveis.

Art. 22 Todos os serviços da instituição, como páginas de internet, correio eletrônico, sistemas de gestão, aplicativos de dispositivos móveis, entre outros, devem possuir tecnologias de autenticação e criptografia que garantam a integridade, o sigilo e a autenticidade das informações.

CAPÍTULO V
DA GESTÃO DE RISCOS E TRATAMENTO DE INCIDENTES

Art. 23 A STI deve identificar os processos necessários para buscar a eliminação, redução, ou transferência de riscos aos dados e serviços da UFS, levando em consideração sua viabilidade estratégica e econômica.

Art. 24 A STI deve difundir noções de segurança da informação para os usuários no âmbito da UFS.

Art. 25 A STI deve possuir uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades a serem desempenhadas.

Art. 26 Os incidentes de segurança, assim como as providências tomadas, devem ser comunicados à STI, que os encaminhará à ETIR.

Art. 27 A ETIR será responsável por tratar as notificações relacionadas aos incidentes de Segurança da Informação.

Art. 28 Para evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação e comunicações causados por incidentes de segurança, a STI deverá manter um Plano de Gerenciamento de Incidentes, elaborado e alinhado ao Programa de Gestão de Continuidade de Negócios.

Art. 29 A UFS deve adotar processo contínuo de gestão de riscos de segurança da informação, que deve ser revisto e atualizado periodicamente pela STI a fim de se precaver quanto a riscos advindos de novas tecnologias e ameaças.

Art. 30 Cabe à STI criar e atualizar o Plano de Tratamento de Riscos.

Art. 31 Cabe à STI definir e pôr em prática as medidas necessárias para a preservação da segurança dos serviços e servidores institucionais sob sua responsabilidade.

Art. 32 A UFS deve manter soluções de proteção contra problemas de segurança lógica, como vírus, invasões, entre outros, definidas pela STI.

Art. 33 Durante o gerenciamento dos incidentes de segurança, qualquer indício de ilícitos criminais deve ser comunicado pela STI ao CGD para avaliação das providências cabíveis.

CAPÍTULO VI
DA CONTINUIDADE DE NEGÓCIO

Art. 34 Cabe à STI criar e atualizar o Programa de Gestão da Continuidade de Negócios, com o intuito de evitar situações de interrupção e manter o funcionamento dos sistemas de informação e comunicação da universidade.

Art. 35 Para os sistemas de atividade crítica, deverão ser contratados serviços ou utilizados equipamentos que disponham de recursos de redundância de processamento, de armazenamento de

dados, de sistemas elétricos, etc, bem como, controle de estabilidade da corrente elétrica, temperatura, umidade e acesso físico restrito.

Art. 36 Os servidores computacionais, onde se encontram os sistemas de atividade crítica, devem estar em sala segura contra problemas de segurança física, como incêndios, enchentes, acesso não autorizado, entre outros.

Art. 37 No caso de hospedagem de serviços dentro das instalações da UFS, a subestação de energia e refrigeração do ambiente onde se encontram estes sistemas deve garantir o seu pleno funcionamento, devendo a STI enviar relatório anual ao gestor de segurança da informação, com o quadro da situação destes.

Art. 38 O código-fonte dos sistemas de informação desenvolvidos pela STI deve ser gerenciado por ferramenta específica de controle de versão, que deve permitir a identificação do responsável pela inclusão/exclusão/alteração do código-fonte, assim como a recuperação de versões recentes.

Art. 39 O acesso à ferramenta específica de controle de versão deverá ser restrito através de perfis de acesso específicos e registrados em trilhas de auditoria.

Art. 40 O ambiente destinado à execução dos sistemas e o ambiente de produção não devem ser utilizados para testes.

Art. 41 O ambiente de testes deve estar separado dos demais ambientes.

Art. 42 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.

Art. 43 Ambientes de produção devem estar separados de demais ambientes lógicos e ter seu acesso reservado apenas a usuários internos responsáveis pela implantação dos sistemas de informação.

Art. 44 Cabe à STI a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalação e recuperação de softwares, sistemas operacionais e sistemas de gerenciamento de banco de dados, de forma a garantir ambientes lógicos que não comprometam a segurança da informação ou contenham vulnerabilidades.

CAPÍTULO VII
DO CONTROLE E UTILIZAÇÃO DE ACESSO

Art. 45 Cabe à STI garantir a segurança das informações institucionais na rede acadêmica da UFS, limitando os acessos, lógicos e físicos, a usuários autorizados e assegurando a operação segura dos recursos, devendo ser considerados os seguintes aspectos:

I. O acesso aos ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário;
II. Sempre que houver a admissão, mudança das atribuições ou desligamento de colaboradores na UFS, será responsabilidade da chefia imediata notificar os gestores dos ativos, para que possam providenciar as ações necessárias relacionadas a suspensão dos privilégios de acesso aos respectivos ativos;
III. Todo o ambiente da UFS deve ser classificado e protegido com mecanismos adequados de segurança, de acordo com a criticidade e o sigilo dos ativos que estão sendo mantidos.

Art. 46 A concessão de acesso aos ativos de informação da UFS tem por objetivo permitir apenas a execução das atividades acadêmicas: ensino, pesquisa, extensão e administração.

Art. 47 As contas de acesso são únicas, individuais, intransferíveis, equivalentes à assinatura do usuário e possuem nível de delegação para desempenho das funções do usuário.

Art. 48 Os usuários com vínculo ativo na universidade podem solicitar uma conta de correio eletrônico com domínio da universidade: @ufs.br ou @academico.ufs.br.

Art. 49 O endereço de correio eletrônico é concedido pela universidade exclusivamente para fins institucionais e não deve ser utilizado para a prática de atos ilícitos, isto é, proibidos pela Lei ou por normas e diretrizes da universidade, que lesionem os direitos e interesses da universidade ou de terceiros.

Art. 50 A STI deverá possuir mecanismos de controles de acesso às informações e aos recursos de processamento de informação que garantam a segurança, a integridade e a disponibilidade dos dados.

Art. 51 As trocas de informações, tanto internamente quanto externamente, deverão ser reguladas de modo a manter um nível adequado da segurança.

Art. 52 A troca de dados em meios informatizados deve ser monitorada e armazenada em *logs*, para que seja possível detectar atividades não autorizadas.

Art. 53 O acesso remoto aos recursos computacionais da UFS deve ser realizado mediante autorização prévia da STI e adoção dos mecanismos de segurança definidos pela STI para evitar ameaças à integridade e ao sigilo do serviço.

Art. 54 A equipe de suporte da STI poderá acessar de forma remota as estações de trabalho dos usuários, mediante solicitação destes ou em razão de demandas próprias da STI, exclusivamente para fins de execução de serviços relacionados aos sistemas computacionais autorizados ou homologados na UFS.

Art. 55 O acesso à rede de internet da universidade deve ser feito mediante credenciais exclusivas do usuário e sua utilização é reservada para fins institucionais e não para a prática de atos ilícitos, isto é, proibidos pela Lei ou por normas e diretrizes da universidade, que lesionem os direitos e interesses da universidade ou de terceiros.

Art. 56 O acesso às bases de dados dos ambientes de produção deve ser feito através dos sistemas de informação, ou por acesso direto feito por usuário responsável pela base e com registro que permita identificar a modificação feita e a autoria da modificação.

Art. 57 Com o intuito de preservar a utilização dos serviços da UFS para atividades pertinentes e garantir a segurança digital, é permitido à STI realizar auditoria e monitoramento das atividades dos usuários nos recursos e serviços TIC no âmbito da UFS.

Art. 58 Havendo evidência de atividade capaz de comprometer a segurança recursos ou dados no âmbito da UFS, a STI está livre para inspecionar arquivos e registros de acessos, restringir acessos, remover dados, desativar servidores, ou implementar filtros de segurança.

CAPÍTULO VIII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 59 A execução dos procedimentos relacionados à segurança da informação da UFS deve ser provida pela STI.

Art. 60 Aos usuários com acesso aos ativos de informação da UFS compete:

I. Cumprir com a POSIC e normas complementares, atos e ações decorrentes da sua implementação;
II. Comunicar formalmente à ETIR qualquer incidente ou ameaça à Segurança da Informação de que tiver ciência;
III. Participar das ações de capacitação relacionadas à segurança de informação promovidas ou divulgadas pela UFS.

Art. 61 É responsabilidade de Terceiros e Fornecedores de serviços que envolvam ativos de informação para a UFS:

I. A proteção dos ativos físicos e lógicos da UFS que estejam sob sua guarda, evitando perda ou modificação de dados, software e hardware;
II. Assegurar o retorno dos serviços inerentes aos ativos de informação em situações de falha, além da eliminação da informação e dos ativos ao final do contrato ou em dado momento previamente definido;
III. Observar restrições em relação a cópias e divulgação de informações, além dos acordos de confidencialidade;
IV. Relatar incidentes ou violação de segurança da informação à ETIR da UFS;
V. Atender aos princípios e diretrizes desta POSIC, incluindo as normas e atos complementares relacionadas à segurança da informação.

Art. 62 Após sua publicação, é de responsabilidade da STI promover a divulgação da POSIC aos usuários no âmbito da UFS.

Art. 63 As normas definidas em prol da segurança da informação devem ser respeitadas e seguidas por todos os usuários no âmbito da UFS.

Art. 64 A aprovação de alterações é feita pelo CGD da UFS.

Art. 65 Nos editais de licitação, contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para UFS, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, principalmente, aqueles que envolvam ativos de informação.

Art. 66 Devem existir acordos de confidencialidade ou de não divulgação para proteger os dados de usuários da UFS, sempre que terceirizados ou fornecedores de serviço tiverem acesso a dados sigilosos da universidade.

Art. 67 São vedados o armazenamento, compartilhamento e a divulgação de dados pessoais ou sensíveis sob a posse da Universidade com qualquer ente que não possa ser responsabilizado por meio de contrato ou convênio com a UFS.

CAPÍTULO IX
DAS VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 68 Atos ou ações que violam esta política, ou suas normas complementares, ou prejudicam de alguma forma o controle de segurança da informação da UFS, serão apurados mediante processo administrativo disciplinar.

Art. 69 Ao(s) responsável(is) pela violação à política serão aplicadas sanções e penalidades previstas na legislação em vigor.

CAPÍTULO X
DA POLÍTICA DE ATUALIZAÇÃO

Art. 70 Propostas de alteração da POSIC devem ser encaminhadas à STI.

Art. 71 Esta política deverá ser revisada anualmente pela STI e atualizada conforme a necessidade, mesmo que em período inferior.

Art. 72 Esta política deverá ser complementada pela STI com a elaboração de normas e procedimentos complementares necessários para a utilização dos serviços de Tecnologia da Informação por ela oferecidos a toda comunidade acadêmica.

CAPÍTULO XI
DISPOSIÇÕES FINAIS

Art. 73 A versão vigente da POSIC e suas normas e procedimentos complementares de segurança de utilização dos serviços ficam disponíveis para consulta na página da *web* da STI.

Art. 74 A utilização dos serviços e recursos TIC no âmbito da UFS implica na aceitação desta política e de normas complementares e no comprometimento com sua preservação.

Art. 75 Os casos omissos serão tratados pelo CGD da UFS.

Art. 76 A presente política entra em vigor a partir da data de sua publicação.