POSIC

Política de Segurança da Informação e Comunicação

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO N. 836, DE 16 DE DEZEMBRO DE 2021

Aprova a Política de Segurança da Informação e Comunicação (POSIC), no âmbito da Universidade Federal do Pará (UFPA).

O REITOR DA UNIVERSIDADE FEDERAL DO PARÁ, no uso das atribuições que lhe conferem o Estatuto e o Regimento Geral, em cumprimento à decisão da Colenda Câmara de Legislação e Normas e do Egrégio Conselho Universitário, em Reunião Ordinária realizada em 16.12.2021, e em conformidade com os autos do Processo n. 041939/2021 – UFPA, procedentes do Centro de Tecnologia da Informação e Comunicação (CTIC), promulga a seguinte

R E S O L U Ç Ã O :

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicação (POSIC), no âmbito da Universidade Federal do Pará (UFPA), na forma do anexo (páginas 2 - 13), que é parte integrante e inseparável desta Resolução.

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

Reitoria da Universidade Federal do Pará, em 16 de dezembro de 2021.

EMMANUEL ZAGURY TOURINHO
R e i t o r
Presidente do Conselho Universitário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

CAPÍTULO I
DOS OBJETIVOS

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

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

Art. 2º Esta POSIC e suas Normas Complementares aplicam-se a todas as unidades e subunidades vinculadas à UFPA, bem como aos servidores, alunos, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação da UFPA.

CAPÍTULO II
DAS DEFINIÇÕES

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

I – Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II – Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III – Ativo: tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal (APF);

IV – Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V – Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VI – Capacitação em Segurança da Informação e Comunicação: saber o que é segurança da informação e comunicação, aplicando-a em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização como gestor de SIC;

VII – Capacitação: visa à aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigidos para o exercício das funções;

VIII – Comitê de Segurança da Informação e Comunicação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de SIC;

IX – Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados;

X – Conscientização em SIC: saber o que é Segurança da Informação e Comunicação, aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

XI – Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

XII – Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIII – Custodiante: responsável por armazenar e preservar as informações que não lhe pertencem, mas que estão sob sua custódia;

XIV – Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XV – Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

XVI – Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias

para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XVII – Gestão de Segurança da Informação e Comunicação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicação;

XVIII – Gestor de Segurança da Informação e Comunicação: é responsável pelas ações de segurança da informação e comunicação no âmbito do órgão ou entidade da APF;

XIX – Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XX – Informação Estratégica: toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos;

XXI – Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXII – Nível de Segurança Adequado: será estabelecido em documentos complementares a esta POSIC;

XXIII – Política de Segurança da Informação e Comunicação (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicação;

XXIV – Terceiro: pessoa, não integrante do órgão ou entidade da APF, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXV – Proprietário da Informação: pessoa ou setor que produz a informação;

XXVI – Quebra (Comprometimento) de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e da comunicação;

XXVII – Riscos de Segurança da Informação e Comunicação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXVIII – Segurança da Informação e Comunicação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXIX – Segurança de Operações e Comunicação: responsável pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta;

XXX – Sensibilização em SIC: saber o que é Segurança da Informação e Comunicação, aplicando tais conhecimentos em sua rotina pessoal e profissional;

XXXI – Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada, para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXXII – Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

XXXIII – Lei Geral de Proteção de Dados (LGPD): estabelecida pela Lei nº 13.709, de agosto de 2018, a LGPD entrou em vigor em setembro de 2020 e dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

XXXIV – CSIRT: Grupo técnico de resposta e tratamento de incidentes de segurança computacional;

XXXV – Computação em nuvem ou *cloud computing*: termo que define os serviços computacionais (hardware e/ou software) hospedados em provedores fora da

infraestrutura física da instituição e que são acessados a partir da Internet.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º O conjunto de documentos que compõem esta POSIC deverá se guiar pelos seguintes princípios:

I – Menor privilégio: usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

II – Segregação de função: funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

III – Auditoria: todos os eventos significativos de sistemas e processos devem ser rastreáveis até o evento inicial;

IV – Mínima dependência de segredos: os controles deverão ser efetivos, ainda que a ameaça saiba de sua existência e como eles funcionam;

V – Controles automáticos: sempre que possível, controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano;

VI – Resiliência: os sistemas e processos devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VII – Defesa em profundidade: controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

VIII – Exceção aprovada: exceções à POSIC deverão sempre ter indicação do Comitê de Segurança da Informação e Comunicação e aprovação do Comitê de Governança Digital ou colegiado equivalente;

IX – Substituição da segurança em situações de emergência: controles somente devem ser desconsiderados de formas pré-determinadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

Parágrafo único. Esta POSIC deve estar, também, em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal (APF), bem como aos demais dispositivos legais aplicáveis.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

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

Art. 6º Os custos associados à Gestão da SIC deverão ser compatíveis com os custos dos ativos de informação que se deseja proteger.

Art. 7º A gestão de SIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos de informação, possibilitando alcançar os objetivos estratégicos da UFPA, assim como otimizar seus investimentos.

Art. 8º As normas e procedimentos de SIC da UFPA, devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de Segurança da Informação e Comunicação.

CAPÍTULO V
GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 9º Os ativos de informação da organização são elementos fundamentais para a consecução dos objetivos estratégicos, portanto ações de segurança específicas deverão garantir a proteção adequada dos mesmos. Os níveis de proteção devem variar de acordo com a criticidade do ativo para a UFPA.

Art. 10. De forma a evitar incidentes de segurança que possam danificar a imagem da Instituição e interromper suas operações, os ativos de informação devem ter controles de segurança implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção ou destruição.

Art. 11. De forma a garantir o entendimento e a prática efetiva da SIC, as

pessoas, que de alguma forma tenham acesso aos ativos de informação da organização, devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

Art. 12. Os processos e atividades que sustentam os serviços críticos disponibilizados pela UFPA devem ser protegidos de forma a garantir a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade (DICA) das informações.

Parágrafo único. Quanto a sua localização, os ativos de informação poderão estar presentes na infraestrutura de rede institucional da UFPA, por exemplo, os hospedados em seu data center principal ou em unidades que possuam capacidade técnica de hospedagem, como também disponibilizados e acessados através de computação em nuvem. Ambas as formas devem estar alinhadas à Lei Geral de Proteção de Dados (LGPD).

CAPÍTULO VI
GESTÃO DE RISCOS

Art. 13. Com o objetivo de reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da organização, deverá ser estabelecido processo que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

CAPÍTULO VII
GESTÃO DE OPERAÇÕES E COMUNICAÇÃO

Art. 14. Dada a importância estratégica que os recursos de processamento da informação têm para a consecução dos objetivos desta Universidade, ações de segurança deverão garantir a operação segura e correta desses recursos.

Art. 15. As interfaces com terceiros são importantes canais de informação que, sem um nível de segurança adequado, poderão levar a organização a uma elevada exposição a riscos. Com o objetivo de reduzir os riscos associados, o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços.

Art. 16. A troca de informações, tanto internamente quanto externamente, deverá ser regulada de forma a manter o nível adequado de segurança.

Art. 17. Visando detectar, o mais cedo possível, atividades não autorizadas, as operações deverão ser adequadamente verificadas.

CAPÍTULO VIII
CONTROLE DE ACESSOS

Art. 18. O objetivo de evitar incidentes de segurança, devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações.

Art. 19. É condição necessária para o acesso aos ativos de informação desta Universidade, a concordância aos preceitos desta POSIC, conforme norma complementar.

Art. 20. Considerando que ambientes de computação móvel e de trabalho remoto são necessários para a consecução das atividades da Universidade e que podem consistir em pontos fracos do sistema de gestão de segurança, devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto.

CAPÍTULO IX
GESTÃO DE INCIDENTES E DE CONTINUIDADE DO NEGÓCIO

Art. 21. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da Universidade.

Art. 22. A interrupção das atividades desta Universidade leva à suspensão de serviços críticos prestados ao cidadão e poderá resultar em grave dano à imagem da organização. Portanto, deverão ser instituídas normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio, para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços da UFPA, além de recuperar perdas de ativos de informação a um nível estabelecido, por intermédio de ações de

prevenção, resposta e recuperação.

Art. 23. A UFPA deve instituir, grupo técnico para tratamento, resposta e prevenção de incidentes de segurança computacional, seguindo a Norma Complementar nº 05/IN01/DSIC/GSIPR que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais nos órgãos e entidades da APF.

CAPÍTULO X
CONSONÂNCIA E RESPONSABILIDADES

Art. 24. O cumprimento desta Política de Segurança deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas pelo Comitê de Segurança da Informação e Comunicação.

Art. 25. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares, tendo por base as conformidades com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 26. Devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da APF, de forma a obter o absoluto cumprimento destes instrumentos legais e normativos.

Art. 27. É de responsabilidade da Administração Superior desta Universidade prover a orientação e o apoio necessários às ações da SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

Art. 28. É de responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes desta política no âmbito de suas áreas de atuação.

Art. 29. É de responsabilidade de todos que têm acesso aos ativos de informação da Universidade manter níveis de segurança da informação adequados, segundo preceitos desta política e de suas normas complementares.

CAPÍTULO XI
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 30. O Comitê terá como atribuições mínimas:

I – assessorar na implementação das ações de Segurança da Informação e Comunicação;

II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre a SIC;

III – propor alterações na POSIC;

IV – propor normas relativas à Segurança da Informação e Comunicação.

Art. 31. O Comitê será a instância competente para dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC desta Universidade.

CAPÍTULO XII
GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 32. O Gestor de SIC será o Coordenador do Comitê de Segurança da Informação e Comunicação e terá como atribuições mínimas:

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

II – acompanhar as investigações e as avaliações dos incidentes de segurança;

III – propor recursos necessários às ações de segurança da informação e comunicação;

IV – realizar e acompanhar estudos e novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicação;

V – manter contato direto com o Departamento de Segurança da Informação e Comunicação (DSIC) para o trato de assuntos relativos à segurança da informação e comunicação;

VI – propor normas relativas à Segurança da Informação e Comunicação;

VII – coordenar a Gestão de Riscos de Segurança da Informação e Comunicação;

VIII – coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes de Segurança (ETRIS ou CSIRT, na sigla em inglês);

IX – buscar apoio para prover os meios necessários para a capacitação e o

aperfeiçoamento técnico dos membros da ETRIS (CSIRT); e

X – implementação dos procedimentos relativos ao uso dos recursos criptográficos, em conformidade com as orientações contidas na Norma Complementar vigente.

CAPÍTULO XIII
PROPRIETÁRIO E CUSTODIANTES DOS ATIVOS DE INFORMAÇÃO

Art. 33. Os níveis adequados de segurança dos ativos de informação deverão ser garantidos pelos proprietários e custodiantes diretamente responsáveis pelos mesmos.

CAPÍTULO XIV
PENALIDADES, ATUALIZAÇÕES E VIGÊNCIAS

Art. 34. Incidentes que violem a POSIC serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 35. Processo disciplinar específico deverá ser elaborado para apurar as ações que constituem comprometimento das diretrizes impostas por esta POSIC.

Art. 36. Esta POSIC, bem como os documentos gerados a partir dela, deverão ser revisados e atualizados preferencialmente a cada dois anos, ou quando mudanças significativas ocorrerem.

CAPÍTULO XV
DISPOSIÇÕES GERAIS

Art. 37. Esta POSIC, bem como as normas e procedimentos de Segurança da Informação e Comunicação associados, deverão ter ampla divulgação, de forma a garantir que todos entendam suas responsabilidades e ajam de acordo com os preceitos desta Política.

Art. 38. Os casos omissos ou não previstos nesta política serão tratados pelo Comitê de Governança Digital;

Art. 39. A presente Política de Segurança da Informação e Comunicação entrará em vigor a partir da data de sua publicação.

Art. 40. Os seguintes documentos são necessários para disciplinar a Governança de TIC e a segurança da informação institucional como parte do conjunto de ações necessárias à ampliação e aplicação da Política de Segurança da Informação e Comunicação da UFPA, sem prejuízo da atualização e proposição de outros atos normativos:

I – Política de Governança de TIC;

II – Política de Gestão de ativos de TIC;

III – Política de Gestão de Serviços de TIC;

IV – Política de Backup e Restauração de Dados Institucionais;

V – Política Organizacional de Desenvolvimento de Software;

VI – Instrução normativa de hospedagem de soluções de TIC;

VII – Instrução normativa sobre utilização do E-mail institucional;

VIII – Instrução normativa sobre utilização e acesso aos recursos de TIC;

IX – Instrução normativa sobre a utilização do Google para educação;

XI – Instrução normativa sobre a utilização do Microsoft Office para educação;

XII – Plano de gestão de continuidade de negócio;

XIII – Plano de gestão de incidentes de TIC;

XIV – Plano de gestão de risco de TIC;

XV – Plano de gestão de mudanças;

XVI – Plano de gestão de configuração;

XVII – Plano de adequação a LGPD;

XVIII – Plano de dados abertos.