UNIVERSIDADE FEDERAL DE PERNAMBUCO

CONSELHO DE ADMINISTRAÇÃO

RESOLUÇÃO Nº 05/2022

Estabelece a Política de Segurança da Informação da Universidade Federal de Pernambuco.

O **CONSELHO DE ADMINISTRAÇÃO** DA UNIVERSIDADA FEDERAL DE PERNAMBUCO, no uso de suas atribuições que lhe confere o Art. 20, inciso XI do Estatuto,

CONSIDERANDO:

- o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), e que dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

- a Lei 9.609 de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências;

- a Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da presidência da Republica (GSI/PR), que aprova o Glossário de Segurança da Informação;

- a Instrução Normativa nº 03, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgão e nas entidades da administração pública federal;

- a Instrução Normativa do Gabinete de Segurança Institucional da presidência da Republica (GSI/PR) nº 1, de 27 de maio de 2020, que dispõe sobre a estrutura de gestão da segurança da informação nos órgãos e nas entidades da administração pública federal;

- a Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta ou indireta;

- a Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que disciplina as diretrizes para a implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta ou indireta;

- a Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta ou indireta;

- a Norma ABNT NBR ISSO/IEC 27001:2006 – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;

- a Norma ABNT NBR ISSO/IEC 27002:2005 – Técnicas de Segurança – Código de Práticas para a Segurança da Informação;

- a Norma ABNT NBR ISSO/IEC 27005:2008 – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação; e

- a apreciação da proposta pelo Comitê de Tecnologia da Informação e Comunicação – CTIC, em reunião realizada no dia 14 de dezembro de 2021 e no dia 07 de abril de 2022.

RESOLVE:

CAPITULO I

DAS DISPOSIÇOES PRELIMINARES

Art. 1º Estabelecer a Política de Segurança da Informação (POSIN) da Universidade Federal de Pernambuco (UFPE), observados os princípios, objetivos e diretrizes contidos nesta resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

§ 1º A POSIN estabelece as orientações e diretrizes corporativas gerais de segurança e controle dos ativos de informação da UFPE ou sob sua guarda, objetivando sua proteção e a prevenção de responsabilidade legal para todos os usuários.

§ 2º Integram também a POSIN normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinadas à proteção dos ativos de informação e à disciplina de sua utilização, emanados no âmbito da UFPE.

Art. 2º A estrutura da segurança da informação da UFPE é integrada por três instrumentos normativos, de níveis hierárquicos distintos, relacionados a seguir:

I - Política de Segurança da Informação (POSIN): define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;

II - Normas de Segurança da Informação (NSI): identificam obrigações e procedimentos em conformidade com as diretrizes da POSIN, a serem seguidas em todas as situações em que a informação é tratada; e

III - Procedimentos de Segurança da Informação (PSI): instrumentalizam os dispositivos, permitindo a direta aplicação nas atividades da UFPE.

Art. 3º A POSIN irá se alinhar às estratégias da UFPE e terá por objetivo garantir os princípios de segurança das informações produzidas ou custodiadas pela UFPE, abrangendo aspectos físicos, tecnológicos e humanos da organização.

Art. 4º A POSIN e as normas de segurança da informação devem ser divulgadas a todos os usuários da UFPE e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Parágrafo único. Os procedimentos de segurança da informação devem ser divulgados apenas às áreas relacionadas à sua execução.

CAPÍTULO II

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 5º Para os efeitos da POSIN e das normas por ela originadas, entende-se por:

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, observada eventual restrição que se aplique;

II - Agente responsável: servidor público ou empregado ocupantes de cargo efetivo que se enquadre em qualquer das opções seguintes:

a) possuidor de credencial de segurança;

b) incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

c) incumbido de chefiar ou gerenciar o processo de Inventário e Mapeamento de Ativos de informação;

d) incumbido de chefiar e gerenciar o uso de dispositivos móveis; e

e) incumbido da gestão do uso seguro de redes sociais;

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

IV - APF: Administração Pública Federal;

V - Atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzam ou suportem um ou mais produtos ou serviços;

VI - Ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

VII - Comitê de Tecnologia da Informação e de Comunicação: tem por finalidade acompanhar e avaliar os serviços relacionados à tecnologia da informação, segurança da informação ou riscos de TIC e comunicação na UFPE.

VIII - Controle, proteção ou contramedida: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

IX - Custodiante do ativo de informação: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

X - Desastre: evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

XI - Equipe de Tratamento de Incidentes em Segurança da Informação (ETISI): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidente de segurança em computadores;

XII - Gestão de continuidade de negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização, e suas atividades de valor agregado;

XIII - Gestão de riscos de segurança da informação e comunicações: conjunto de processos que permitem 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;

XIV - Gestor da informação: qualquer servidor ou unidade que, no exercício de suas competências, é responsável pela produção de informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues à UFPE;

XV - Gestor de segurança da informação: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da APF;

XVI - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

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

XVIII - Plano de continuidade de negócios: documento dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

XIX - Plano de gerenciamento de incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XX - Plano de recuperação de negócios: documento dos procedimentos e de informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas à normalidade;

XXI - Plano de tratamento dos riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

XXII - Programa de gestão da continuidade de negócios: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis, e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;

XXIII - Recurso: é um meio de qualquer natureza (humano, físico, tecnológico, financeiro, de imagem de mercado, de credibilidade, entre outros) que permite alcançar aquilo a que se propõe;

XXIV - Resiliência: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre e retornar à normalidade de operações;

XXV - Riscos de segurança da informação: 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;

XXVI - Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXVII - Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXVIII - Trilhas de auditoria: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento;

XXIX - Usuário externo: pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativa ou academicamente à UFPE;

XXX - Usuário interno: pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativa ou academicamente à UFPE;

XXXI - Usuários: pessoa física seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade;

CAPÍTULO III

DOS ATRIBUTOS E DOS PRINCÍPIOS

Art. 6º A segurança da informação, coberta pela presente POSIN, terá, dentre outros inerentes à administração pública federal, os seguintes atributos:

I - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

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

III - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; e

IV - 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.

Art. 7º A presente POSIN terá, dentre outros inerentes à administração pública federal, os seguintes princípios:

I - Responsabilidade: preservação da integridade e tratamento de maneira adequada, de acordo com sua classificação, da informação, bem como preservar e zelar pelos ativos de informação;

II - Clareza: as regras que se fundam nesta POSIN devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão; e

III - Publicidade: transparência às informações, respeitando a privacidade do cidadão.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 8º A segurança da informação deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação.

Art. 9º Os dirigentes das unidades e demais chefias da UFPE assumem o compromisso de atuar junto à Coordenação de Segurança da Informação e Proteção de Dados (CSIPD) da Superintendência de Tecnologia da Informação (STI) e à Equipe de Tratamento de Incidentes de Segurança da Informação (ETISI), naquilo que por ventura sejam solicitados, bem como de desenvolver suas atividades de forma colaborativa em estrita observância as orientações determinadas pela CSIPD/ETISI, naquilo que tange a segurança da informação, objetivando minimizar as vulnerabilidades e ameaças que possam comprometer o negócio da instituição.

Art. 10. A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 11. A autoridade máxima da UFPE é responsável por garantir os recursos necessários para a execução da Política de Segurança da Informação dentro da disponibilidade orçamentária.

Seção I

Do Tratamento Da Informação

Art. 12. Todo ativo de informação sob a responsabilidade da UFPE é considerado um bem e deve ser protegido pela instituição, de acordo com as diretrizes descritas nesta POSIN, a Lei Geral de Proteção de Dados Pessoais - LGPD e demais regulamentações em vigor, com o objetivo de minimizar os riscos aos serviços e atividades, bem como preservar a imagem institucional.

Art. 13. A classificação da informação obedecerá às diretrizes estabelecidas pela Lei de Acesso à Informação – LAI – regulamentada pelo Decreto nº 7.724/2012, do Governo Federal ou documento correspondente que venha a substituí-lo.

Seção II

Da Gestão de Incidentes em Segurança da Informação

Art. 14. Para evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação causados por incidentes de segurança, a STI deverá manter um Plano de Gestão de Incidentes em Segurança da Informação, elaborado e alinhado ao Programa de Gestão de Continuidade de Negócios, conforme a Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009.

Art. 15. Todo incidente de segurança da informação, bem como suas providências, deverá ser comunicado à CSIPD, que de acordo com a criticidade do incidente, deverá comunicar ao Gestor de Segurança da Informação da UFPE.

Seção III

Da Gestão de Riscos

Art. 16. A STI deve adotar processo contínuo de Gestão de Riscos de Segurança da Informação – GRSI, conforme estabelecido na Instrução Normativa IN DSIC-GSI/PR Nº 3 de 28 de maio de 2021, ou documento correspondente que venha a substituí-lo.

Art. 17. O processo de GRSI deverá ser revisto periodicamente pela STI, com a participação da CSIPD/ETISI e demais diretorias da STI, a fim de aperfeiçoar e agir proativamente contra riscos advindos de novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.

Art. 18. Caberá à STI a criação e atualização do Plano de Tratamento de Riscos, com a participação da CSIPD/ETISI e demais diretorias da Superintendência.

Seção IV

Da Gestão de Continuidade

Art. 19. Com o objetivo de evitar situações de interrupção e manter em funcionamento os sistemas de informação da UFPE, a STI com a participação da CSIPD/ETISI e demais diretorias da STI, deverá manter um Programa de Gestão da Continuidade de Negócios, conforme a IN DSIC-GSIPR Nº 3 de 28 de maio de 2021.

Seção V

Da Auditoria e Conformidade

Art. 20. A STI deverá propor normas complementares ao CTIC, 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, em conformidade com a Norma Complementar nº 21/IN01/DSIC/GSI/PR, de 8 de outubro de 2014.

Seção VI

Dos Controles de Acesso

Art. 21. A concessão de acesso aos ativos de informação da UFPE tem por objetivo garantir aos usuários a realização de suas atividades.

Art. 22. O uso dos ativos de informação na UFPE, pelos seus usuários, deve ser direcionado prioritariamente para a realização das atividades de ensino, pesquisa, extensão e de administração desempenhadas nos limites da ética, razoabilidade e legalidade.

Art. 23. A conta de acesso e a senha de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representam nível de delegação concedida para o desempenho de suas funções.

Art. 24. A STI deverá normatizar o acesso físico e lógico aos ativos de tecnologia da informação da UFPE, como forma de garantir a sua proteção.

Seção VII

Do Uso de E-mail

Art. 25. Os usuários internos da UFPE terão direito a uma conta de correio eletrônico no serviço de correio eletrônico da instituição, que terá uma única titularidade, determinando a responsabilidade sobre sua utilização.

Art. 26. O usuário deve utilizar a sua conta de correio eletrônico em conformidade com a lei, a moral, os bons costumes e a ordem pública.

Parágrafo único. O e-mail não deverá ser usado para a prática de atos ilícitos – proibidos pela lei ou pela presente diretriz ou normas complementares que venham a ser editadas – lesivas aos direitos e interesses da UFPE ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os ativos de informação, bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

Seção VIII

Do Acesso a Internet

Art. 27. A STI deve propor norma ao CTIC, de forma que seja possível definir procedimentos e implementar mecanismos de autenticação que determinem a titularidade de todos os acessos à internet feitos pelos usuários que estejam sob sua responsabilidade.

Art. 28. Aplica-se ao usuário da Internet o disposto no art. 26 e seu parágrafo único.

Seção IX

Dos Sítios

Art. 29. Os serviços e servidores da instituição tais como os de páginas de Internet, correio eletrônico, sistemas administrativos e sistemas acadêmicos, deverão ser configurados para usar tecnologias de autenticação e criptografia visando a garantir a integridade, o sigilo e a autenticidade das informações.

Art. 30. Caberá à STI definir e pôr em prática as medidas necessárias para preservar a segurança dos serviços e servidores institucionais que estiverem sob sua responsabilidade, de forma a não comprometer a segurança das redes internas e externas à instituição.

Parágrafo único. A unidade que adotar domínio próprio deverá pôr em prática as medidas necessárias para preservar a segurança dos seus serviços e servidores, definidas pela STI, de forma a não comprometer a segurança das redes internas e externas a instituição.

Art. 31. Deve haver pelo menos um responsável para atuar como contato no que se refere à segurança dos serviços e servidores na unidade responsável pelo mesmo.

Seção X

Da Gestão da Segurança da Informação e Comunicações

Art. 32. O processo de Gestão da Segurança da Informação deverá ser proposto pela CSIPD, com a participação da ETISI, e aprovado pelo CTIC em norma complementar.

Seção XI

Da Gestão de Ativos

Art. 33. O processo de Gestão de ativos deve ser desenvolvido em conformidade com as determinações da IN DSIC-GSIPR Nº 3 de 28 de maio de 2021 ou outro documento que venha substituí-la.

Seção XII

Da Segurança Física do Ambiente de TI

Art. 34. Para os sistemas de missão 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 corrente elétrica (rede estabilizada), temperatura, umidade e acesso físico restrito.

Parágrafo único. Cabe ao CTIC classificar os sistemas de missão crítica e a sua definição de proteção, considerando a criticidade das informações e os ativos de informação envolvidos nesses sistemas.

Art. 35. Os servidores computacionais, onde se encontram os sistemas de missão crítica, devem estar em sala segura contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, acesso indevido, entre outros).

Parágrafo único. Cabe à STI a definição de dispositivos ou serviços de proteção, considerando a criticidade das informações e dos ativos de informação envolvidos, e que estejam sob sua responsabilidade.

Art. 36. Cabe à STI providenciar o pleno funcionamento de energia e refrigeração do ambiente onde se encontram os sistemas de missão crítica para a UFPE.

Seção XIII

Da Segurança Lógica do Ambiente de TI

Art. 37. A UFPE deverá manter soluções de proteção contra problemas de segurança lógica (vírus, acesso não autorizado, invasões, desempenho, espaço em disco, etc.), cabendo à STI a definição de tais soluções de proteção, considerando a criticidade dos ativos de informação envolvidos e que estejam sob sua responsabilidade.

Art. 38. Cabe à STI a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalações e recuperação de **softwares**, sistemas operacionais, SGDB, de forma a garantir que estes ambientes lógicos não tragam vulnerabilidades que comprometam a segurança da informação, bem como, propor as normas que regulamentarão tais procedimentos.

Art. 39. Cabe aos órgãos da UFPE providenciar que os ambientes lógicos, sob sua responsabilidade, tenham o seu acesso restrito por senhas seguras, ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela STI.

Seção XIV

Da Segregação de Ambientes

Art. 40. A STI deve assegurar que todos os sistemas de informação, sob sua responsabilidade, estejam aderentes as diretrizes a seguir:

I - segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais;

II - que os ambientes de produção somente poderão ser acessados por usuários internos responsáveis pela implantação e manutenção dos sistemas de informação;

III - que 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, será feito por um membro da equipe responsável pela base de dados com autorização de um usuário interno com nível gerencial da área solicitante e o acesso direto deverá ser registrado em meio que permita a identificação do que foi modificado e quem foi responsável pela modificação;

IV - que os sistemas de informação 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- que o código-fonte dos sistemas de informação deverá ser gerenciado por ferramenta específica de controle de versão, devendo o acesso à ferramenta ser restrito através de perfis de acesso específicos e registrados em trilhas de auditoria e 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 - que o ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não devem ser utilizados para testes e estes devem ser feitos em ambiente apropriado e gerenciado; e

VII - que 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 V

DAS SANÇÕES E PENALIDADES

Art. 41. Atos ou ações que violem o disposto nesta Resolução ou em quaisquer de suas normas e/ou procedimentos complementares, ou que prejudiquem os controles de segurança da informação, no âmbito da UFPE, serão apurados mediante instauração de processo administrativo disciplinar.

Parágrafo único. Os responsáveis por prejuízos ou irregularidades mencionados no **caput** deste artigo responderão administrativa, civil e/ou penalmente pelos seus atos.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 42. A estrutura para a Gestão de Segurança da Informação e Comunicações na UFPE é composta pelo (a):

I - Comitê de Tecnologia da Informação e de Comunicação (CTIC);

II - Gestor de Segurança da Informação;

III - Coordenação de Segurança da Informação e Proteção de Dados (CSIPD); e

IV - Equipe de Tratamento de Incidentes em Segurança da Informação (ETISI).

Seção I

Do Comitê de Tecnologia da Informação e de Comunicação

Art. 43. O CTIC tem por finalidade acompanhar e avaliar os serviços relacionados à tecnologia da informação, segurança da informação ou riscos de TIC e comunicação desenvolvidos na UFPE, observando o disposto em seu Regimento, nas resoluções dos órgãos deliberativos superiores e na legislação federal vigente, em matéria concernente com as suas competências.

Art. 44. As competências do CTIC estão enumeradas no Regimento da Reitoria e, no que tange a segurança da informação, deve estar em conformidade com a Instrução Normativa Nº 1, de 27 de Maio de 2020 do GSI/PR, ou documento correspondente que venha a substituí-lo.

Seção II

Da Presidência e da Secretaria do Comitê

Art. 45. A presidência do CTIC será exercida pelo Gestor de Segurança da Informação.

Parágrafo único. O Superintendente da Superintendência de Tecnologia da Informação será designado pelo Reitor como Gestor de Segurança da Informação.

Art. 46. As atribuições do Presidente do CTIC estão definidas no regimento do CTIC.

Art. 47. A Secretaria do CTIC será exercida por servidor designado pelo Superintendente de Tecnologia da Informação.

Seção III

Do Gestor de Segurança da Informação e Comunicações

Art. 48. O Superintendente da Superintendência de Tecnologia da Informação será designado pelo Reitor como Gestor de Segurança da Informação

Art. 49. Compete ao Gestor de Segurança da Informação:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

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

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 ou na entidade;

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

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

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

IX - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação; e

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

Seção IV

Do Coordenador de Segurança da Informação e Proteção de Dados

Art. 50. O coordenador de segurança da informação da STI será indicado pelo Superintendente de Tecnologia da Informação.

Art. 51. Compete ao Coordenador de Segurança da Informação e Proteção de Dados:

I - promover a cultura de segurança da informação e comunicações;

II - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

III - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança da informação;

IV - manter contato direto com a Diretoria de Governança e Gestão de TIC – DGGTIC e a Superintendência de Tecnologia da Informação – STI para o trato de assuntos relativos à segurança da informação e comunicações;

V - propor alterações na POSIN; e

VI - propor normas relativas à segurança da informação.

Seção V

Da Equipe de Tratamento de Incidentes em Segurança da Informação

Art. 52. A UFPE deverá manter Equipe de Tratamento de Incidentes em Segurança da Informação – ETISI e, no seu documento de constituição adotar as recomendações do Anexo A da Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, ou documento correspondente que venha a substituí-lo.

Parágrafo único. A ETISI é instituída por portaria normativa expedida pelo Reitor, devendo ser atualizada quando necessário.

Seção VI

Dos Gestores de Informação

Art. 53. São responsabilidades dos gestores da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:

I - adotar as medidas e procedimentos necessários para garantir a segurança das informações;

II - definir procedimentos, critérios de acesso e classificar as informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes, considerando os procedimentos da Lei de Acesso à Informação – LAI, e o Serviço de Informação ao Cidadão – SIC, no âmbito da UFPE;

III - propor regras específicas ao uso das informações;

IV - manter o devido registro e controle ao autorizar e fornecer acesso aos ativos de TI sob sua responsabilidade aos usuários; e

V - observar as diretrizes da Lei Geral de Proteção de Dados Pessoais – LGPD.

§ 1º As informações recebidas de pessoa física ou jurídica externa à universidade serão submetidas, adicionalmente, às medidas de segurança da informação e proteção dos dados compatíveis com os requisitos pactuados com quem as forneceu.

§ 2º O Reitor, os Pró-Reitores, os Superintendentes e os Diretores de unidade podem indicar orientar e autorizar, a qualquer tempo, procedimentos que visem a garantir a segurança da informação e proteção dos dados, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

Seção VII

Do Custodiante da Informação

Art. 54. São responsabilidades do custodiante da informação:

I - garantir a segurança da informação e proteção dos dados sob sua custódia;

II - comunicar oportunamente ao CTIC sobre situações que comprometam a segurança das informações e a proteção dos dados sob sua custódia;

III - comunicar ao CTIC eventuais limitações para cumprimento dos critérios definidos para segurança da informação e proteção dos dados; e

IV - observar procedimentos, critérios de acesso e classificação das informações definidos pelos Gestores da Informação.

Seção VIII

Dos Dirigentes das Unidades e Demais Chefias

Art. 55. São responsabilidades dos dirigentes e demais chefias das unidades da UFPE no que se refere à segurança da informação:

I - conscientizar os usuários sob sua supervisão em relação aos conceitos e às praticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;

IV - avaliar os danos, para sua área, decorrentes de quebra de segurança; e

V - tomar as providências cabíveis quando da comunicação conclusiva do incidente encaminhada pelo CTIC.

Seção IX

Dos Usuários de Ativos de Informação

Art. 56. É dever de todos os usuários de ativos de informação:

I - conhecer e cumprir as diretrizes e normas desta POSIN;

II - responsabilizar-se por todo e qualquer acesso aos ativos de informação da UFPE, bem como pelos efeitos desse acesso, realizado por meio de seu código de identificação;

III - comunicar o mais breve possível os incidentes de segurança da informação, por ele conhecido, ao setor responsável; e

IV - colaborar com as investigações de incidentes, envolvendo direta ou indiretamente sua área.

Seção X

Do Relacionamento com Terceiros

Art. 57. Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para UFPE, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIN.

Parágrafo único. No caso de contratação de produto ou serviço de TIC faz-se necessário incluir requisitos de segurança da informação e privacidade conforme orientação do Guia de Requisitos e de Obrigações quanto à Segurança da Informação e Privacidade ou documento que venha a substituí-lo.

CAPÍTULO VII

DAS DISPOSIÇÕES TRANSITÓRIAS, GERAIS E FINAIS

Art. 58. Esta resolução deverá ser revisada e atualizada a cada 2 (dois) anos, a contar da sua vigência ou quando identificada a necessidade pelo CTIC.

Art. 59. Os casos omissos nesta resolução serão decididos pelo presidente do CTIC, ouvidos, quando for o caso, os membros do referido comitê.

Art. 60. As diretrizes da POSIN serão implementadas de forma incremental, conforme projeto de implantação aprovado pelo CTIC.

Art. 61. O projeto de implantação da POSIN será desenvolvido em conjunto pelas unidades da STI, e liderado pela DGGTIC/CSIPD, da Superintendência.

Art. 62. Fica revogada a Resolução nº 01/2017, do Conselho de Administração.

Art. 63. Esta Resolução entra em vigor em 1º de agosto de 2022.

APROVADA NA 3ª (TERCEIRA) SESSÃO ORDINÁRIA DO CONSELHO DE ADMINISTRAÇÃO DA UNIVERSIDADE FEDERAL DE PERNAMBUCO, REALIZADA NO DIA 21 DE JULHO DE 2022.

Presidente: **Prof. ALFREDO MACEDO GOMES**
Reitor