Ministério da Educação
Universidade Federal do Piauí
Gabinete do Reitor

RESOLUÇÃO CONSUN/UFPI Nº 49 DE 22 DE DEZEMBRO DE 2021

Altera a Resolução Nº 061/13, de 10 de dezembro de 2013, que dispõe sobre a Política de Segurança da Informação da Universidade Federal do Piauí.

O REITOR DA UNIVERSIDADE FEDERAL DO PIAUÍ-UFPI e PRESIDENTE DO CONSELHO UNIVERSITÁRIO-CONSUN, no uso de suas atribuições legais, estatutárias e regimentais, e considerando:

- as competências que lhe foram atribuídas pelo Regimento do Conselho Universitário, desta Universidade, aprovado pela Resolução nº 01/1984, de 15 de fevereiro de 1984 e alterado pela Resolução nº 27/2013, de 16 de abril de 2013;

- a decisão do Conselho Universitário em reunião do dia 20 de dezembro de 2021;

- o Processo Nº 23111.07407/2021-85;

- a Lei nº 13.709, de 14 de agosto de 2018;

- a Lei nº 12.527, de 18 de novembro de 2011;

- o Decreto nº 9.832, de 12 de Junho de 2019;

- o Decreto nº 9.637, de 26 de Dezembro de 2018;

- o Decreto nº 7.845, de 14 de Novembro de 2012;

- a Instrução Normativa GSI nº 1, de 27 de maio de 2020;

- a Instrução Normativa GSI nº 2, de 24 de julho de 2020;

- a Normativa Complementar 04/DSIC/GSIPR de 15 de Fevereiro de 2013;

- a Normativa Complementar 05/DSIC/GSIPR de 14 de Agosto de 2009;

- a Normativa Complementar 06/DSIC/GSIPR de 11 de Novembro de 2009;

- a Normativa Complementar 07/DSIC/GSIPR de 14 de Julho de 2014;

- a Normativa Complementar 08/DSIC/GSIPR de 19 de Agosto de 2010;

- a Normativa Complementar 10/DSIC/GSIPR de 30 de Janeiro de 2012;

- a Normativa Complementar 11/IN01/DSIC/GSIPR, de 10 de Fevereiro de 2012;

- a Normativa Complementar 18/IN01/DSIC/GSIPR, de 10 de Abril de 2013;

- a Normativa Complementar 19/IN01/DSIC/GSIPR, de 15 de Julho de 2014;

- a Normativa Complementar 20/IN01/DSIC/GSIPR, de 15 de Dezembro de 2014; e

- o Glossário de Segurança da Informação, aprovado pela Portaria nº 93, de 26 de Setembro de 2019.

RESOLVE:

Art. 1º A Resolução Nº 061/13, de 10 de dezembro de 2013, passa a vigorar com as seguintes alterações:

> "Art. 1° Esta Resolução regulamenta a política de segurança da informação, que determina as diretrizes a serem seguidas no tratamento da segurança dos recursos computacionais e informações geradas no âmbito da Universidade Federal do Piauí.
>
> Art. 2º A política de segurança da informação da Universidade Federal do Piauí tem os seguintes objetivos:
>
> I - apresentar de forma clara a visão desta instituição, e de sua administração superior, relacionada à Segurança da Informação e Comunicação;
>
> II - instituir princípios e diretrizes de Segurança da Informação e Comunicação no âmbito da Universidade Federal do Piauí com o propósito de limitar a exposição ao risco e garantir a disponibilidade, a integridade, a confidencialidade, a autenticidade e não repúdio das informações e comunicações que suportam os objetivos estratégicos e atividades de ensino, pesquisa e extensão desta Universidade; e
>
> III - servir de referência para auditoria, apuração e avaliação de responsabilidades.
>
> Art. 3º Esta política e suas eventuais normas complementares aplicam-se às unidades administrativas e acadêmicas da Universidade Federal do Piauí, conforme o Estatuto da Universidade Federal do Piauí, abrangendo toda a comunidade universitária integrada pelos corpos docentes, discentes e técnicos administrativos e a quem de alguma forma, tenha acesso aos ativos de informação da instituição
>
> Art. 4º O quadro de alterações desta política encontra-se no Anexo Único desta resolução.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

CAPÍTULO I

CONCEITOS E DEFINIÇÕES

Art. 5º Considerando o disposto no art. 6º da Instrução Normativa GSI No 1, de 27 de maio de 2020, que orienta os órgãos e as entidades da Administração Pública Federal a fazerem uso do Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos, para efeito desta política serão adotadas as seguintes definições:

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 ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta e indireta, que se enquadre em qualquer das opções seguintes: possuidor de credencial de segurança; incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; incumbido de chefiar ou gerenciar o processo de Inventário e Mapeamento de Ativos de informação; incumbido de chefiar e gerenciar o uso de dispositivos móveis; incumbido da gestão do uso seguro de redes sociais;

III - ativo: qualquer coisa que tenha valor para esta instituição;

IV - ativo 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;

V - ataque: ação que constitui uma tentativa deliberada e não autorizada para acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível;

VI - **backup** ou Cópia de Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VII - capacitação: atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicação, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de Segurança da Informação e Comunicação;

VIII - classificação do ativo: definição do nível de segurança adequado para um ativo;

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

IX - conformidade: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização;

X - conscientização: ações educativas que impactam na mudança de postura e de comportamento com relação a Segurança da Informação e Comunicação;

XI - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XII - CTIR Gov: Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal. Responsável pelo atendimento aos incidentes em redes de computadores da Administração Pública Federal;

XIII - custódia: consiste na responsabilidade de se guardar um ativo para terceiros sem, contudo, permitir, automaticamente, o acesso ao ativo ou o direito de conceder acesso a outros;

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

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

XVI - **e-mail** institucional: serviço de correio eletrônico oferecido por esta instituição para seus servidores como instrumento de trabalho;

XVII - ferramentas: conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplica a política de segurança da informação da Universidade Federal Piauí;

XVIII - gestor de ativos: membro desta instituição responsável pela gestão de um determinado ativo;

XIX - gestão de ativos de informação: processo abrangente de gestão que mapeia os ativos de informação institucionais, identificando, no mínimo e de forma inequívoca, seu conjunto completo de informações básicas (nome, descrição e localização), seus respectivos responsáveis (proprietários e custodiantes), seus requisitos legais de negócio, sua classificação, sua documentação, seu ciclo de vida, seus riscos associados e seus controles de Segurança da Informação e Comunicação implementados, bem como os outros ativos de informação relacionados;

XX - gestão de continuidade de negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações da atividade institucional caso essas ameaças se concretizem, de forma a fornecer uma estrutura para que desenvolva uma resiliência organizacional

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

capaz de recuperar perdas de ativos de informação a um nível aceitável pré-estabelecido, por intermédio de ações de prevenção, resposta e recuperação, de forma a salvaguardar os interesses de áreas envolvidas, a reputação, a marca da organização e seus valores agregados;

XXI - gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XXII - gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XXIII - **hardening**: é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e tornando um sistema menos vulnerável a ameaças;

XXIV - incidente: qualquer evento ou ocorrência que promova uma ou mais ações que comprometa, ou que seja uma ameaça à integridade, autenticidade, confiabilidade e disponibilidade de qualquer ativo da Universidade Federal do Piauí;

XXV - informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

XXVI - norma: conjunto de regras que devem ser seguidas por um grupo;

XXVII - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);

XXVIII - tratamento de incidentes: serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

XXIX - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 6º O conjunto de documentos que compõem esta Política de Segurança da Informação deverá guiar-se pelos seguintes princípios de segurança da informação e comunicações:

I - segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

II - menor privilégio: pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

III - auditabilidade: Todos os eventos necessários à garantia da integridade, da confiabilidade e da autenticidade dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;

IV - mínima dependência de segredos: os controles de Segurança da Informação e Comunicações devem ser efetivos para mitigação de riscos e ameaças;

V - controles automáticos: deverão ser aplicados, sempre que possível, controles de segurança automáticos, especialmente aqueles controles que dependem da vigilância humana e do comportamento humano;

VI - resiliência: os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VII - defesa em camadas: controles devem ser desenhados em camadas ou níveis, de tal forma que, se uma camada de controle falhar, exista um tipo diferente de controle em outra camada ou nível para prevenir a exploração das vulnerabilidades de segurança;

VIII - exceção aprovada: exceções à Política de Segurança da Informação devem sempre ser documentadas e ter aprovação superior;

IX - legalidade: respeito à obediência aos princípios constitucionais, administrativos e à legislação vigente; e

X - substituição de segurança em situações de emergência: controles de segurança devem ser desconsiderados somente de formas pré determinadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

CAPÍTULO III

DAS DISPOSIÇÕES GERAIS

Art. 7º A Política de Segurança da Informação deverá ser mantida em concordância com o Plano de Desenvolvimento Institucional que abrange a missão da Universidade, os seus valores, o Projeto Pedagógico Institucional, o processo avaliativo interno e externo e as políticas acadêmicas e de gestão, a infraestrutura existente e projetada.

Art. 8º O modelo de gestão de segurança da informação e comunicações da Universidade Federal do Piauí deverá ser integrado e suportado pelos subsídios gerados pela Gestão de Riscos, Gestão de Ativos, Gestão de Incidentes, Gestão de Continuidade de Negócios e Gestão de Conformidade, em consonância com o especificado nas diretrizes desta Política de Segurança da Informação.

Art. 9º A gestão de segurança da informação e comunicações deve apoiar a tomada de decisões, bem como realizar a gestão de conhecimento e recursos por meio do aproveitamento eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos da Universidade Federal do Piauí, assim como otimizar seus investimentos.

Art. 10 As ações de segurança da informação e comunicações devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade da Universidade Federal do Piauí.

Art. 11 Os custos associados à gestão de segurança da informação e comunicações deverão ser compatíveis com os custos dos ativos que se deseja proteger.

Art. 12 As normas, procedimentos, manuais e metodologia de segurança da informação e comunicações da Universidade Federal do Piauí devem considerar as normas e padrões da Administração Pública Federal como referência nos processos de gestão e governança.

Art. 13 As normas, procedimentos, manuais e metodologia de segurança da informação e comunicações da Universidade Federal do Piauí devem estipular mecanismos que garantam a orientação à conformidade dos controles de segurança da informação e comunicações associados.

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

Art. 15 Deve ser estabelecida a integração entre as instâncias e estruturas de supervisão e apoio definidas nesta Política de Segurança da Informação e aquelas definidas em outras políticas e normas da Universidade Federal do Piauí.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

Seção I

Do tratamento da informação

Art. 16 O tratamento da informação refere-se ao conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 17 Os servidores e demais funcionários deverão observar os princípios desta política quando realizarem o tratamento de informações no âmbito da Universidade Federal do Piauí.

Art. 18 Considerando o disposto na Lei Nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação, a Universidade Federal do Piauí deve assegurar a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação, bem como a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade e a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Art. 19 A Universidade Federal do Piauí deve possuir normas atualizadas relativas à Segurança da Informação e Comunicação, com vistas a gerir, manter, avaliar e atualizar critérios de proteção da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, conforme a legislação em vigor.

Art. 20 No tratamento da informação deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo Federal.

Art. 21 O tratamento da informação classificada no âmbito da Universidade Federal do Piauí seguirá o estabelecido no Decreto Nº 7.845, de 14 de Novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Art. 22 O tratamento de dados pessoais no âmbito da Universidade Federal do Piauí seguirá o estabelecido na Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais.

Seção II

Da segurança física e do ambiente

Art. 23 O acesso físico aos ambientes de Tecnologia da Informação e Comunicação deverá possuir controles e mecanismos de segurança adequados aos níveis de segurança exigidos para cada local.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

Art. 24 As infraestruturas críticas ou sensíveis, os equipamentos, os processos e atividades que sustentam os serviços críticos de Tecnologia da Informação e Comunicação disponibilizados pela Universidade Federal do Piauí, devem ser protegidos considerando os riscos identificados, os níveis de segurança definidos, os controles de segurança implementados, o acesso indevido, os danos e as interferências.

Parágrafo único. As infraestruturas consideradas críticas ou sensíveis ficam definidas como todas as instalações internas do **datacenter**, **racks** de **switches** e depósitos de equipamentos.

Art. 25 Procedimentos para restringir a comida, bebida e fumo dentro ou perto das instalações críticas ou sensíveis, devem ser estabelecidos pela Coordenadoria da Infraestrutura e aprovados pela Autoridade Máxima da Universidade Federal do Piauí.

Parágrafo único. As instalações consideradas críticas ou sensíveis ficam definidas como todas as da área interna do **datacenter** e **racks** de **switches**.

Art. 26 A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e/ou normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação.

Art. 27 Equipamentos instalados fora das áreas de segurança deverão dispor de proteção física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas.

Art. 28 Equipamentos instalados fora dos limites da Universidade Federal do Piauí e interligados a ela, devem ter autorização expressa do agente responsável pela administração da Rede de **Internet** para poder manter a conexão.

Art. 29 Instalações e equipamentos internos não devem ser retirados da Universidade Federal do Piauí sem a devida autorização.

Art. 30 Caso algum indivíduo seja pego cometendo furto, ataque ou destruição de propriedade no âmbito da Universidade Federal do Piauí, deve-se notificar o Departamento de Vigilância para que este entre em contato com as autoridades competentes.

Art. 31 Todas as portas, fechaduras e métodos de acesso que não estejam funcionando em sua plena capacidade devem ser informados à Prefeitura Universitária que realizará correção do artefato defeituoso.

Art. 32 Dispositivos de armazenamento danificados, assim como equipamentos em geral, devem sofrer uma avaliação de riscos, realizada pelo setor responsável, para verificar se eles devem ser destruídos, reparados ou descartados.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

Art. 33 Equipamentos enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e **software** licenciado foi removido ou sobreposto antes da alienação do equipamento.

Art. 34 Todo o sistema de proteção física deverá receber manutenção preventiva semestral ou quando houver necessidade identificada pela Coordenadoria de Infraestrutura.

Seção III

Da gestão de ativos

Art. 35 É de responsabilidade de todos que têm acesso aos ativos da Universidade Federal do Piauí manter os níveis de segurança da informação adequados, segundo preceitos desta Política de Segurança e suas Normas Complementares.

Art. 36 No tratamento dos ativos, que envolve a identificação, classificação, manipulação e conservação, deve ser considerados os seguintes aspectos para todo ativo custodiado ou de propriedade desta instituição:

I - ser inventariado;

II - ser protegido segundo as diretrizes descritas nesta política e nas demais regulamentações em vigor;

III - ter um gestor de ativos, sobre quem recai a responsabilidade sobre a segurança do respectivo ativo;

IV - ser autorizado pelo respectivo gestor do ativo;

V - ser classificado quanto aos aspectos de confidencialidade, integridade, autenticidade, não repúdio e disponibilidade, de forma explícita ou implícita. Esse processo de classificação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada ativo de informação;

VI - ser cedido somente mediante autorização formal. Essa autorização deve observar a classificação do ativo e a legislação vigente; e

VII - ser feita a classificação e cessão pelo respectivo gestor do ativo.

Art. 37 Com relação ao controle de acesso, que envolve o acesso lógico e físico dos ativos, devem ser considerados os seguintes aspectos:

I - todo o uso dos ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de uso deve ser previamente autorizada formalmente pelo respectivo gestor do ativo;

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

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

III - 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; e

IV - as pessoas que possuem acesso aos ativos da instituição devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e tratamento da informação.

Art. 38 Com relação à auditoria e conformidade devem ser considerados os seguintes aspectos para o uso do ativo:

I - deve gerar trilhas de auditoria que devem ser mantidas para efeito de análise; e

II - é passível de monitoramento e auditoria e, sempre que possível, deve ser analisado em busca de indícios de descumprimento desta política.

Art. 39 Os processos e atividades que sustentam os serviços críticos disponibilizados pela Universidade Federal do Piauí devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações.

Seção IV

Da gestão do uso dos recursos operacionais e de comunicações

Art. 40 O uso da **internet** pela comunidade da Universidade Federal do Piauí deve ser realizado de acordo com o disposto na Norma de Uso da Internet da Universidade Federal do Piauí.

Art. 41 O uso do **email** institucional pela comunidade da Universidade Federal do Piauí deve ser realizado de acordo com o disposto na Política de Gerência e Uso do **Email** Institucional na Universidade Federal do Piauí.

Art. 42 O uso de Senhas e Acesso deve ser realizado de acordo com o disposto na Norma de Gerenciamento e Utilização das Senhas de Acesso da Universidade Federal do Piauí.

Art. 43 O uso das Estações de Trabalho pela comunidade da Universidade Federal do Piauí deve ser realizado de acordo com o disposto na Norma de Uso das Estações de Trabalho da Universidade Federal do Piauí.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

Seção V

Da gestão de continuidade de negócio

Art. 44 A Universidade Federal do Piauí deverá estabelecer um Sistema de Gestão de Continuidade de Negócios, homologado pelo Conselho Universitário, a fim de minimizar os impactos decorrentes de potenciais eventos que causem a indisponibilidade dos serviços desta instituição.

Art. 45 Toda forma de tratamento e operação de **backups** desta instituição deve seguir o estabelecido na Política de **Backups** e Restauração da Universidade Federal do Piauí.

Art. 46 Ambientes críticos devem ter seguir as diretrizes do Plano de Gestão de Continuidade de Negócios e seus procedimentos devem ser revisados e testados regularmente.

Seção VI

Da gestão de riscos

Art. 47 A Universidade Federal do Piauí deverá estabelecer um Plano de Gestão de Riscos, proposto dentro do Sistema de Gestão de Continuidade de Negócios, homologado pelo Conselho Universitário, que possibilite a identificação, quantificação, priorização, tratamento, comunicação e monitoração periódica dos riscos.

Art. 48 As unidades administrativas e acadêmicas da Universidade Federal do Piauí, com apoio da Superintendência de Tecnologia da Informação, deverão implementar e executar as atividades de gestão de riscos de Segurança da Informação e Comunicação associadas aos ativos de informação sob sua responsabilidade.

Art. 49 Os riscos de Segurança da Informação e Comunicação deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades administrativas e acadêmicas e dos ativos relacionados, gestores e fiscais de contrato, bem como os fornecedores e custodiantes os responsáveis por manter os níveis apropriados de segurança da informação na entrega dos serviços.

Art. 50 O processo de gestão de riscos será instituído e revisto periodicamente pelo Comitê Gestor de Segurança da Informação da Universidade Federal do Piauí, para prevenção contra riscos advindos de novas tecnologias e ameaças externas, visando à elaboração de planos de ação apropriados.

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

Seção VII

Da gestão de incidentes

Art. 51 A Superintendência de Tecnologia da Informação da Universidade Federal do Piauí deverá criar uma Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação.

Art. 52 A Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação deverá criar e manter uma metodologia para tratamento e resposta a incidentes em redes computacionais, com o objetivo de coordenar as atividades relacionadas a incidentes de segurança em redes de computadores.

Art. 53 A Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação apresentará planos de gerenciamento de incidentes e da ação de resposta a incidentes, a serem aprovados pelo Comitê Gestor de Segurança da Informação e homologados pelo Conselho Universitário.

Art. 54 Os incidentes de segurança da informação deverão ser prontamente reportados por todos os pertencentes ao corpo universitário, de forma sigilosa, às autoridades responsáveis e apurados pela Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação.

Art. 55 Dentre os serviços de tratamento de incidentes, devem estar, no mínimo, as atividades de receber, analisar e responder os incidentes de segurança oriundos do âmbito da Universidade Federal do Piauí.

Art. 56 Os incidentes de segurança da informação recebidos devem ser devidamente registrados e classificados.

Art. 57 O tratamento e resposta a incidentes de de segurança da informação devem guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamentos de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança e Redes de Computadores da Administração Pública Federal.

CAPÍTULO IV

DA AUDITORIA E CONFORMIDADE

Art. 58 O cumprimento desta Política de Segurança da Informação deverá ser avaliado periodicamente, por meio de verificações de auditoria e conformidade realizadas com apoio do Comitê Gestor de Segurança da Informação na Universidade Federal do Piauí.

Art. 59 Os controles de Segurança da Informação e Comunicação devem ser analisados criticamente e verificados em períodos regulares pelo Comitê Gestor de Segurança da Informação, tendo por base a conformidade com políticas,

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 60 Cabe ao Comitê Gestor de Segurança da Informação da Universidade Federal do Piauí instituir processos de auditoria, análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 61 Para o efetivo cumprimento desta política é responsabilidade da Autoridade Máxima desta Instituição:

I - instituir e atualizar o Comitê Gestor de Segurança da Informação;

II - designar o chefe da Divisão de Segurança da Informação;

III - instituir a Divisão de Segurança da Informação;

IV - aprovar a Política de Segurança da Informação; e

V - garantir os recursos necessários para a implementação destas diretrizes.

Art. 62 São responsabilidades do Comitê Gestor de Segurança da Informação desta Instituição:

I - propor, analisar e aprovar normas, procedimentos e soluções específicas que atendam às necessidades de segurança da informação;

II - apoiar a implementação das ações de segurança da informação;

III - analisar os casos relacionados à segurança da informação omissos nesta política; e

IV - desenvolver e implementar um Programa de Conscientização e Capacitação em Segurança da Informação como método auxiliar desta política.

Art. 63 São responsabilidades do chefe da Divisão de Segurança da Informação:

I - dirigir as atividades da Divisão de Segurança da Informação;

II - promover a cultura institucional de Segurança da Informação;

III - propor recursos necessários às ações de Segurança da Informação;

IV - tratar de assuntos relacionados à Segurança da Informação na instituição; e

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

V - assessorar as atividades da Divisão de Segurança da Informação.

Art. 64 São responsabilidades da Divisão de Segurança da Informação:

I - apoiar ações para capacitar e conscientizar os membros desta instituição sobre segurança da informação;

II - desenvolver ações relacionadas à Gestão de Risco, conforme o previsto nesta política;

III - desenvolver ações relacionadas às Auditoria e Conformidade, conforme o previsto nesta política;

IV - monitorar, sempre que possível, os ativos de forma a identificar a ocorrência de incidentes de segurança;

V - definir e executar processo formal para tratar e responder os incidentes de segurança identificados e reportados;

VI - desenvolver ações relacionadas à Gestão de Continuidade, conforme o previsto nesta política;

VII - propor normas e procedimentos seguindo as diretrizes desta política;

VIII - implementar procedimentos, técnicas e boas práticas de **Hardening**; e

IX - auditar o cumprimento desta política bem como das normas e procedimentos ligados a esta política.

Art. 65 São responsabilidades das Chefias desta Instituição:

I - gerenciar o cumprimento da política de segurança da informação, por parte dos seus funcionários;

II - identificar os desvios praticados e adotar medidas corretivas apropriadas;

III - proteger, em nível físico e lógico, os ativos de informação e processamento da Universidade Federal do Piauí relacionados com sua área de atuação;

IV - garantir que o pessoal sob sua supervisão compreenda e colabore com a proteção dos ativos de informação da Universidade Federal do Piauí;

V - sempre se manter atualizada sobre noções básicas de segurança da informação; e

VI - solicitar à Superintendência de Tecnologia da Informação ou à unidade gestora do sistema, a concessão de acesso privilegiado a usuários sob sua supervisão que podem acessar as informações da unidade administrativa sob sua

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**

responsabilidade, respeitados os limites constitucionais das garantias individuais e coletivas.

Parágrafo único. Cada área que detém os ativos de processamento e de informação será responsável por esses ativos, provendo a sua proteção de acordo com as normas e procedimentos previstos nesta Resolução.

Art. 66 São responsabilidades de todo usuário dos ativos de informação desta Instituição:

I - preservar a integridade e guardar sigilo das informações que fazem uso, bem como zelar e proteger os respectivos recursos de tecnologia da informação;

II - cumprir a Política de Segurança da Informação da Universidade Federal do Piauí, sob pena de incorrer nas sanções disciplinares e legais cabíveis explícitas no Capítulo VIII desta Resolução;

III - utilizar os sistemas de informação da Universidade Federal do Piauí e os recursos a ela relacionados apenas para os fins a que se destinam, sendo vedado seu uso em caráter pessoal;

IV - responder por todos e qualquer recurso de Tecnologia da Informação da Universidade Federal do Piauí sob sua responsabilidade, bem como pelos efeitos dos acessos efetivados através do seu código de identificação ou atributo empregado para esse fim; e

V - comunicar ao seu superior imediato qualquer irregularidade ou desvio.

Art. 67 Entendem-se como responsabilidades dos prestadores de serviço, toda e qualquer ação prevista em contrato ou cláusulas que contemplem o cumprimento da Política de Segurança da Informação da Universidade Federal do Piauí e suas normas e procedimentos.

CAPÍTULO VI

DAS PENALIDADES

Art. 68 Fica assegurada a garantia individual e coletiva dos discentes, docentes e servidores públicos da Universidade Federal do Piauí à inviolabilidade da sua intimidade ao sigilo da correspondência (inclusive as correspondências eletrônicas) e das comunicações nos termos previstos na Constituição Federal.

Art. 69 A quem descumprir os procedimentos previstos nesta política, serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo, aprovado pelo Decreto nº 1171, de 22 de junho de 1994; na Lei nº 8.112, de 11 de dezembro de 1990, que institui o Regime Jurídico Único dos Servidores Públicos Civis da União, das Autarquias, inclusive as em Regime Especial, e das Fundações Públicas Federais, nos artigos 153, §1º (A divulgação de segredo), 154-A (Invasão de

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Bra
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: www.ufpi.br

dispositivo informático), 168 (Apropriação indébita), 266 (Interrupção ou perturbação de serviço informático), 313-A (Inserção de dados falsos em sistemas de informação) e 313-B (Modificação ou alteração não autorizada de sistema de informação), do Código Penal Brasileiro, aprovado pelo Decreto nº 2.848, de 7 de dezembro de 1940, e do art. 927 (ato ilícito e reparação de dano) do Código Civil Brasileiro, aprovado pela Lei nº 10.406, de 10 de janeiro de 2002.

CAPÍTULO VII

DA ATUALIZAÇÃO

Art. 70 Esta política e os instrumentos normativos gerados a partir dela devem ser revisados sempre que necessário, contando que não exceda o período máximo de 04 (quatro) anos.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 71 Esta política deverá ser amplamente publicada e divulgada, garantindo que todos tenham consciência da mesma, para usufruírem dos benefícios e assumirem as responsabilidades inerentes aos sistemas de informação da Universidade Federal do Piauí.

Art. 72 Os casos omissos a esta política serão resolvidos pelo Comitê de Segurança da Informação da Universidade Federal do Piauí., ouvido o Conselho Universitário.

……/……." (NR).

Art. 2º Fica revogada a Resolução 061/13, de 10 de dezembro de 2013.

Art. 3º Esta Resolução entrará em vigor no dia 01 de janeiro de 2022, conforme disposto nos incisos I e II do art. 4º, do Decreto nº 10.139, de 28 de novembro de 2019, da Presidência da República.

Teresina, 22 de dezembro de 2021.

GILDÁSIO GUEDES FERNANDES
Reitor

Campus Universitário "Ministro Petrônio Portella" CEP 64049-550 – Teresina – Piauí – Brasil
Telefones: (86) 3215-5511/3215-5512/3215-5514 – Fax (86) 3237-1812/3237-1216 – Internet: **www.ufpi.br**