MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
COMITÊ DE GOVERNANÇA ESTRATÉGICO

RESOLUÇÃO NORMATIVA Nº 6/2022 - CGE (11.24.10.03)

Nº do Protocolo: 23077.108893/2022-66

Natal-RN, 16 de agosto de 2022.

Aprova a Política de Segurança da Informação e Comunicação da Universidade Federal do Rio Grande do Norte.

O VICE-PRESIDENTE DO COMITÊ DE GOVERNANÇA ESTRATÉGICO DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE, usando das competências previstas no artigo 16, §§ 1º e 3º, da Resolução 13/2022-CONSAD, de 14 de julho de 2022.

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet);

CONSIDERANDO a Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Lei nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;

CONSIDERANDO o Decreto 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;

CONSIDERANDO o Decreto nº 10.332, de 28 de abril de 2020, que institui a estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

CONSIDERANDO a Instrução Normativa GSI/PR nº 1, de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDDERANDO a Instrução Normativa GSI/PR nº 3, de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública;

CONSIDERANDO a determinação contida no art. 85, § 2º, da Resolução 13/2022-CONSAD, de 14 de julho de 2022, para o Comitê de Governança Estratégico aprovar Política de Segurança da Informação e Comunicação da Universidade; e

CONSIDERANDO o que consta no processo nº 23077.106453/2022-74.

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação - POSIC da Universidade Federal do Rio Grande do Norte.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de Segurança da Informação e Comunicação - POSIC da UFRN é uma declaração formal da Instituição acerca do seu compromisso com a proteção dos ativos de informação, físicos e de software, de sua propriedade e/ou sob sua guarda.

Art. 3º O objetivo da POSIC é estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos de informação, servindo de apoio à alta administração da instituição na implementação da gestão de segurança da informação e comunicação, buscando assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

Art. 4º O escopo da POSIC envolve aspectos estratégicos, estruturais, organizacionais e humanos, bem como elementos físicos e lógicos, preparando a base para elaboração dos demais documentos normativos.

Art. 5º A POSIC deve ser cumprida por todos que tenham acesso a quaisquer ativos de informação, físicos e de software, de sua propriedade e/ou sob sua guarda.

Art. 6º Para os fins desta Resolução, considera-se:

I - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição;

II - ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

III - ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

IV - ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

V - ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

VI - auditoria: atividade de avaliação dos registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos à rede interna e à internet;

VII - comunidade universitária: representa os docentes, técnico-administrativos e estudantes da UFRN;

VIII - comunicação: refere-se a transmissão de dados;

IX - incidente de segurança: qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de Segurança da Informação;

X - Recursos de Tecnologia da Informação e Comunicação - RTIC: equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas unidades da instituição, tais como:

a) equipamentos de informática e de telecomunicações de qualquer espécie;

b) infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie; e

c) recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional da UFRN, redes ou outros sistemas de informação.

XI - serviço de rede: processo de software que estabelece conexões de rede para fornecer armazenamento, manipulação, apresentação e/ou transmissão de dados ou outra capacidade;

XII - unidade administrativa: qualquer instância administrativa da UFRN a exemplo dos campi, unidades ligadas aos campi, núcleos de pesquisa e centros com funcionalidades específicas; e

XIII - usuário da Informação: todos que tenham acesso a ativo físico, de informação e de software.

CAPÍTULO II

DOS PRINCIPIOS

Art. 7º A POSIC da UFRN é guiada pelos seguintes princípios, além dos princípios da administração pública:

I - criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

II - responsabilidade: refere-se ao cumprimento de normas de segurança da informação e comunicação pelos usuários da informação para a proteção de cada ativo e pelo cumprimento de processos de segurança;

III - ciência: refere-se ao conhecimento pelos usuários da informação das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IV - ética: todos os direitos e interesses legítimos dos usuários da informação devem ser respeitados; e

V - proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação na UFRN serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

Art. 8º Para o contexto dos serviços, recursos e informações gerenciadas na infraestrutura de Tecnologia da Informação e Comunicação da UFRN, considera-se os seguintes preceitos básicos de segurança da informação:

I - integridade;

II - confidencialidade;

III - disponibilidade;

IV - autenticidade; e

V - irretratabilidade.

CAPÍTULO III

DAS DIRETRIZES GERAIS

Art. 9º São diretrizes gerais da POSIC:

I - estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura da UFRN, bem como ao Plano Diretor de Tecnologia da Informação e Comunicação;

II - estabelecer medidas e procedimentos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e

III - observar as boas práticas e procedimentos de Segurança da Informação e Comunicação recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões.

Art. 10. As diretrizes de segurança da informação definidas nesta política são aplicadas aos ativos de informação, físicos e de software, devendo servir de orientação para instrumentos táticos e operacionais a serem observados pelos usuários da informação.

Art. 11. É dever de todos os usuários da informação zelar pela Segurança da Informação e Comunicação.

Art. 12. A UFRN, como usuária dos serviços providos pela Rede Nacional de Pesquisa - RNP é, por princípio, signatária de suas Políticas e Normas de Segurança.

Seção I

Das diretrizes para o tratamento de ativos

Art. 13. Os ativos deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista sempre que ocorrerem fatos que justifiquem sua atualização.

§ 1º A documentação dos ativos deverá fornecer subsídios para a sua recuperação após um desastre.

§ 2º As regras de documentação dos ativos serão definidas em normas específicas.

Art. 14. Os ativos de um setor deverão ser de responsabilidade do seu gestor, ou de alguém por ele designado, que ficará encarregado pela sua manutenção e documentação, bem como pela notificação de qualquer evento que aconteça.

Art. 15. A instituição deverá adotar as medidas necessárias para que os responsáveis pelos ativos possam geri-los adequadamente, cabendo ao gestor do ativo solicitar os recursos necessários para o gerenciamento.

Seção II

Dos ativos de informação

Art. 16. As informações existentes no âmbito da UFRN apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente.

Art. 17. Normas complementares estabelecerão procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

Art. 18. Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores, dispositivos móveis, dispositivos de armazenamento externo, entre outros) são de sua responsabilidade, cabendo adotarem as medidas necessárias para realizar as cópias de segurança desses ativos e proceder à sua recuperação em caso de perda.

Seção III

Dos ativos de software

Art. 19. A utilização de ativos de software em equipamentos da instituição deve ser previamente autorizada pelo seu responsável, conforme art. 14, a quem compete providenciar os procedimentos necessários à sua utilização.

Art. 20. É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir as disposições desta POSIC, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes.

Seção IV

Dos ativos físicos

Art. 21. Cabe ao responsável pelo ativo a elaboração de procedimentos para o seu uso e controle, devendo ainda zelar pelo cumprimento destes procedimentos.

Seção V

Dos serviços de rede

Art. 22. Os serviços de rede no ambiente da UFRN também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem definidos em normas específicas.

CAPÍTULO IV

DAS DIRETRIZES ESPECÍFICAS

Seção I

Do tratamento de incidentes de segurança da informação e comunicação

Art. 23. A UFRN manterá permanentemente um núcleo de tratamento e resposta a incidentes de segurança da informação e comunicação com a responsabilidade de receber, filtrar, classificar e responder às solicitações e alertas, além de realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa.

Seção II

Da gestão de riscos

Art. 24. A UFRN deverá elaborar e manter Plano de Gestão de Riscos com base na legislação vigente, contendo necessariamente, lista das ameaças mais prováveis e suas ocorrências, classificação dos riscos e alternativas para mitigá-los.

Seção III

Da gestão de continuidade

Art. 25. A UFRN deve adotar um conjunto de procedimentos emergenciais mediante a definição de um Sistema de Gestão de Continuidade de Negócios - SGCN, para a eventualidade da ocorrência de algum incidente de segurança da informação que possa causar interrupção na continuidade de processos organizacionais para a UFRN, decorrentes de desastres ou falhas em recursos de tecnologia da informação e comunicação.

Seção IV

Da auditoria

Art. 26. Todos os ativos de informação, ativos de software, ativos físicos e serviços de rede no âmbito da UFRN são passíveis de auditoria técnica a cargo da Superintendência de Tecnologia da Informação, segundo plano a ser estabelecido em norma específica.

Parágrafo único. Cabe ao Comitê de Governança Estratégico - CGE aprovar plano de auditoria e conformidade, que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta POSIC, no âmbito da UFRN.

Seção V

Do controle de acesso

Art. 27. O objetivo do controle de acesso é limitar as ações que o usuário legítimo de um sistema pode efetuar, buscando prevenir a realização de atividades que venham ocasionar algum incidente de segurança.

Art. 28. Deve ser definido Plano de Controle de Acesso que estabeleça procedimentos para a identificação dos ativos de informação, físicos e de software, com acesso controlado, assim como dos usuários que devem ter privilégio de acesso as áreas físicas protegidas contra o acesso de pessoas não autorizadas.

Seção VI

Do uso de correio eletrônico institucional

Art. 29. Todos os membros da comunidade universitária possuirão um endereço de correio eletrônico institucional.

Art. 30. O serviço de correio eletrônico institucional será usado para atividades acadêmicas e administrativas dos usuários da informação no âmbito da UFRN.

Art. 31. As responsabilidades, direitos e penalidades referentes ao uso de correio eletrônico institucional serão especificadas em normas complementares.

Seção VII

Do acesso e publicação de informações na internet

Art. 32. O acesso à Internet no âmbito da UFRN é fornecido para fins diretos e complementares às atividades da instituição, sendo, portanto, passível de registro e auditoria.

Art. 33. Perfis de redes sociais, sites e portais específicos pertencentes às unidades organizacionais da UFRN devem ser criados, atualizados e descontinuados sob a anuência do gestor responsável pela unidade, devendo, preferencialmente, estar registrado em um domínio da UFRN.

Art. 34. O conteúdo acessado ou publicado não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários/imagens que possam ofender alguém por sua raça, classe social, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou condição de deficiência.

Art. 35. Não é permitida a utilização de conteúdos de terceiros, sujeitos às leis de direito autoral ou classificados como segredo, sem autorização escrita, em qualquer tipo de publicação on-line pertencente às unidades organizacionais da UFRN.

Seção VIII

Da capacitação e aperfeiçoamento

Art. 36. Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em segurança da informação e comunicação.

Seção IX

Da utilização de equipamentos particulares/privados

Art. 37. Equipamentos particulares e/ou privados, como computadores ou quaisquer dispositivos, que possam armazenar e/ou processar dados, não devem ser usados para armazenar e/ou processar informações que sejam classificadas como sensíveis para a atividade da UFRN, sem prévia autorização expressa do custo diante dos dados ou da Direção da Unidade.

Seção X

Dos cuidados com o posto de trabalho

Art. 38. Nenhuma informação sensível deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Seção XI

Das conversas em locais públicos, redes sociais e outros meios

Art. 39. Não se deve discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de qualquer tipo em redes sociais ou qualquer outro meio que não garanta sigilo.

Seção XII

Do termo de responsabilidade e sigilo

Art. 40. O Termo de Responsabilidade e Sigilo é o documento oficial de comprometimento que deve ser firmado por todos os usuários da informação na UFRN.

Art. 41. Como linhas gerais para a confecção do Termo de Responsabilidade e Sigilo, seus signatários devem assumir o compromisso de:

I - declarar o conhecimento e aceitação dos termos desta POSIC e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

II - declarar estar ciente que os acessos realizados por meio da estrutura de Tecnologia da Informação e Comunicação da UFRN são passíveis de auditoria; e

III - manter a confidencialidade de suas credenciais, notificando a UFRN sempre que existir qualquer indício de possível comprometimento para que sejam tomadas as providências cabíveis.

Art. 42. A assinatura do Termo de Responsabilidade e Sigilo deve preceder do consentimento livre e esclarecido.

CAPÍTULO IV
DAS COMPETÊNCIAS DOS USUÁRIOS DA INFORMAÇÃO

Art. 43. Compete aos usuários da informação:

I - conhecer e cumprir os princípios, diretrizes e responsabilidades desta POSIC, bem como normas e resoluções complementares;

II - zelar pela segurança da informação e comunicação;

III - comunicar os incidentes de segurança da informação conhecidos; e

IV - propor melhorias à segurança da informação e comunicação no âmbito da UFRN.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 44. A desobediência ou violação às regras da Política de Segurança da Informação e Comunicação da UFRN e suas normas complementares aprovadas pelo Comitê Gestor de Tecnologia da Informação implicará em sanções administrativas nos termos da lei e normas complementares, sem prejuízo de outras previstas nas esferas cível e penal.

Art. 44. A POSIC e as normas complementares de segurança da informação devem ser amplamente divulgadas a todos os usuários da informação da UFRN.

Art. 45. As referências legais e normativos complementares relacionados à segurança da informação e comunicação são apresentadas em anexo a esta Resolução.

Art. 46. Os casos omissos e as dúvidas surgidas na aplicação do disposto na POSIC deverão ser tratados pelo Comitê de Governança Estratégico - CGE.

Art. 47. Esta Resolução entra em vigor na data de sua publicação.

(Assinado digitalmente em 19/08/2022 09:28)
HENIO FERREIRA DE MIRANDA
VICE-PRESIDENTE
DEDFIS/CCS (15.11)
Matrícula: ###74#6