MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC

RESOLUÇÃO Nº 10 / 2024 - CETIC (11.00.04)

Nº do Protocolo: 23006.014035/2024-57

Santo André-SP, 25 de julho de 2024.

Atualização da Política de Segurança da Informação e Comunicações no âmbito da UFABC.

O COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CETIC) da FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC (UFABC), no uso de suas atribuições legais,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações (POSIC) no âmbito da UFABC, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Art. 2º Esta política tem como objetivo principal instituir as diretrizes estratégicas, as normas complementares, as responsabilidades e as competências para a efetiva gestão da segurança da informação no âmbito da UFABC.

Art. 3º A POSIC será complementada por normas, regulamentos e procedimentos técnicos que a referencie.

Art. 4º Os padrões e regras originadas desta política e as suas normas subsequentes são aplicáveis a toda comunidade acadêmica e demais usuários que tenham acesso às informações custodiadas pela UFABC, envolvendo todas as etapas do seu ciclo: a criação, o manuseio, o transporte, o armazenamento e o descarte, em qualquer meio. Parágrafo único. Em casos específicos, as regras serão aplicáveis somente a subgrupos de usuários da UFABC, sendo que a norma deverá explicitar tal informação.

Art. 5º O cumprimento desta política da segurança e comunicações e de suas normas complementares poderá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê Estratégico de Tecnologia da Informação e Comunicação - CETIC, buscando a certificação do cumprimento dos requisitos de segurança da informação e comunicações e garantia de cláusula de responsabilidade e sigilo.

Art. 6º Para fins desta Resolução, entende-se por:

I. Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal (APF), com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e Comunicações;

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

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

IV. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

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

órgão ou entidade;

VI. Privacidade: a garantia da inviolabilidade dos dados dos usuários, tanto por agentes externos quanto por internos, com exceção dos casos previstos na legislação vigente;

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

VIII. Tratamento da Informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

IX. Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Autenticidade.

X. Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

XI. Ativos de Informação: são os meios de armazenamento, transmissão e processamento, os sistemas de informação, em suporte físico ou digital, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, por exemplo, recursos computacionais, sala de datacenter, sistema acadêmico, senhas, sistema de correio eletrônico, perfis em redes sociais, sítios da internet, entre outros;

XII. Gestor de Segurança da Informação e Comunicações (GSIC): responsável pelas ações de Segurança da Informação e Comunicações no âmbito da UFABC;

XIII. Comitê de Segurança da Informação e Comunicações (CSIC): grupo de pessoas com a responsabilidade de assessorar o CETIC nas ações de Segurança da Informação e Comunicações no âmbito da UFABC;

XIV. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações; XV. Norma de Segurança: documento formalmente aprovado pelo CETIC que prevê regras, diretrizes ou características para as ações de Segurança da Informação e Comunicações no âmbito da UFABC;

XVI. Procedimento de Segurança: documento ou rotina aprovado pelo GSIC que contém a forma ou método de se executar as normas;

XVII. Usuário: Docentes, discentes regulares e especiais dos cursos de graduação ou pós-graduação, participantes de cursos de extensão, servidores técnico-administrativos, estagiários e pesquisadores, desde que cadastrados e ativos no sistema, devendo ser vinculado a pelo menos uma unidade administrativa da UFABC;

XVIII. Colaborador: Prestador de serviço terceirizado ou contratado temporário, vinculado a uma unidade administrativa, que tenham necessidade de acesso às informações tramitadas no âmbito da UFABC;

XIX. Interesse do serviço: necessidade de acesso motivado pelo efetivo serviço do seu cargo ou função.

XX. Controles de acesso físico ou lógico: Sistemas que realizam a concessão ou negação de acesso aos recursos computacionais, documentos e demais ativos de informação, a fim de evitar a quebra de segurança das informações e comunicações.

Art. 7º A Gestão de Segurança da Informação e Comunicações da UFABC deverá observar os seguintes requisitos legais e normativos:

I. Artigo 207 da Constituição Federal;

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. 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;

IV. Decreto nº 8.135, de 04 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

V. Portaria Interministerial dos Ministérios de Planejamento, Orçamento e Gestão, das Comunicações e da Defesa, nº 141 de 02 de maio de 2014, que dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal;

VI. Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008;

VII. Norma Complementar nº 03 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009;

VIII. Lei nº 12.527, de 18 de novembro de 2011 Lei de Acesso à Informação LAI.

IX. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

X. Acórdão do Tribunal de Contas da União nº 1233/2012 de 23 de maio de 2012 que avalia se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

XI. Acórdão do Tribunal de Contas da União nº 1739 de 15 de Julho de 2015 que faz a identificação de riscos relevantes em contratações de serviços de Tecnologia da Informação, sob o modelo de computação em nuvem.

Art. 8º A Gestão da Segurança da Informação e Comunicações na UFABC é norteada pelos seguintes princípios:

I. Autonomia didático-científica: a UFABC reconhece a autonomia didáticocientífica da sua comunidade e, por isso, a gestão da segurança da informação e comunicações não deve prejudicar ou impedir suas atividades-fim.

II. Importância: A UFABC reconhece a importância das Tecnologias da Informação e Comunicação e que seu uso permeia todas as suas atividades, incluindo ensino, pesquisa, extensão, gestão, comunicação interpessoal e lazer;

III. Responsabilidade: toda a comunidade de usuários da UFABC é responsável pelo cumprimento das normas de Segurança da Informação e Comunicações. Além disso, cada ativo de informação deve possuir um responsável;

IV. Legalidade: as ações de Segurança da Informação e Comunicações levarão em consideração as leis, as políticas, as normas e os procedimentos organizacionais, administrativos, técnicos e operacionais da UFABC, formalmente estabelecidos; e

V. Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações na UFABC serão adequados ao entendimento administrativo e/ou acadêmico e ao valor do ativo a proteger.

VI. Menor Privilégio: Qualquer usuário deve ter acesso somente ao necessário para a realização do seu trabalho, para evitar exposições desnecessárias que possam aumentar o nível de risco de segurança;

VII. Transparência: Publicidade das ações de TIC, salvo em hipóteses de sigilo previstas em lei. Das Diretrizes Gerais Art.

Art. 9º A informação é um ativo primário da UFABC que suporta as atividades de ensino, pesquisa, extensão e administração, através de diversos sistemas que viabilizam o cumprimento da sua missão institucional e, para tanto, deve ser classificada adequadamente e protegida quanto aos aspectos de integridade, disponibilidade, autenticidade e confidencialidade.

Art. 10. Deverá ser instituída uma equipe com perfil técnico compatível para compor a ETRISI, que será responsável pelas atividades de resposta a incidentes de Segurança da Informação e Comunicações no âmbito da UFABC.

Art. 11. A gestão de riscos deverá ser prevista no planejamento estratégico de tecnologia da informação e comunicações, que deverá ser orientada pela Política de Gestão de Riscos Corporativos da UFABC e pela Política de Governança de TIC;

Art. 12. A gestão de continuidade dos negócios deverá ser prevista em um plano de continuidade de negócios para manter a disponibilidade dos serviços de tecnologia de informação e comunicações, incluindo o uso de redundância em sua implantação e a definição de planos de contingência para cada cenário de indisponibilidade de sistemas, informações e processos críticos. Parágrafo único. O Núcleo de Tecnologia da Informação tem a prerrogativa de definir as ações necessárias para garantir a continuidade do negócio dos sistemas institucionais.

Art. 13. O controle de acesso dar-se-à da seguinte forma:

I. O nível de privilégio de acesso aos ambientes de tecnologia da informação concedido aos usuários deve ser apropriado ao interesse do serviço, ou seja, à sua necessidade de uso inerente ao efetivo serviço do seu cargo ou função.

II. As senhas de acesso físico e lógico aos ativos de informação da UFABC são de uso pessoal e intransferível.

III. Os locais onde se encontram os ativos de informação devem ter proteção e controle de acesso físico ou lógico compatível com o seu nível de criticidade.

IV - Os dispositivos utilizados para acessar a rede ou sistemas da UFABC em regime de teletrabalho deverão possuir requisitos mínimos de segurança, conforme disposto em normativo específico sobre este tema, a ser elaborado e mantido atualizado e divulgado pelo órgão de gestão de TIC.

Parágrafo único: Este normativo não deverá restringir acesso de dispositivos com sistemas operacionais abertos.

V - A interligação de dispositivos de rede (como switches, roteadores, ou outros dispositivos configurados de maneira a oferecer acesso à rede) à rede da UFABC só poderá ser realizada mediante conhecimento e autorização expressa do órgão de gestão de TIC. Essa permissão tem como objetivo garantir a segurança, integridade e funcionalidade da rede e dos recursos de tecnologia da informação disponibilizados pela Universidade.

Art. 14. O uso dos ativos de informação deverá observar a premissa geral de que estes ativos devem ser utilizados de maneira responsável, devendo este uso estar alinhado prioritariamente com os objetivos educacionais, de pesquisa, extensão, administrativos e gerenciais da Universidade.

Parágrafo único. O uso desses ativos exige que cada um dos usuários assuma a responsabilidade de proteger os direitos da comunidade, de forma que nenhum usuário ou atividade possa prejudicar o uso da comunidade como um todo.

Art. 15. Quanto ao desenvolvimento interno de softwares administrativos, as áreas responsáveis da UFABC devem respeitar as boas práticas de desenvolvimento e engenharia de software preconizados pelo Sistema de Informática do Serviço Público (SISP) do Ministério de Planejamento Desenvolvimento e Gestão (MPDG), os padrões estabelecidos pelo escritório de projetos e processos do NTI, os padrões de interoperabilidade e acessibilidade, as diretrizes de continuidade de negócios desta política, de forma a evitar perda de dados

Art 16. O órgão de gestão de TIC será incumbido de implementar medidas de monitoramento de acesso e utilização da rede corporativa e realizar ações restritivas ao acesso a aplicativos, sites e conteúdos web que possam apresentar riscos à segurança da informação dos dados e dos usuários na rede da UFABC.

§1º Uma normativa de uso seguro da internet será formalizada pelo CETIC, estabelecendo as diretrizes e procedimentos a serem seguidos pela comunidade universitária, visando minimizar tais riscos e promover uma navegação consciente e responsável.

§2º O CSIC decidirá sobre os escopos de restrição e monitoramento aplicados pelo orgão gestor de TI.

Art. 17. O órgão gestor de TIC poderá conduzir campanhas de teste de segurança, treinamentos, e conscientização.

Paragrafo único: os usuários que estiverem envolvidos em incidentes de segurança, poderão ser convidados a realizar treinamento indicado pelo CSIC, visando fortalecer a resiliência e a conscientização sobre as ameaças cibernéticas e protocolos de segurança estabelecidos

Art. 18. Instituir, no âmbito da UFABC:

I. Gestor de Segurança da Informação e Comunicações (GSIC) que deverá ser um servidor designado pelo Reitor, ouvido o CETIC;

II. Comitê de Segurança da Informação e Comunicações (CSIC) que deverá ser composto por membros indicados pelo CETIC.

Paragrafo único: As nomeações devem ocorrer com a maior celeridade possível, sendo facultado à presidência do CETIC a nomeação *ad referendum,* para posterior apreciação em reunião do CETIC.

Das Competências

Art.19. Compete ao Gestor de Segurança da Informação e Comunicações (GSIC):

I. Promover a cultura de Segurança da Informação e Comunicações;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor os recursos necessários às ações de Segurança da Informação e Comunicações;

IV. Coordenar a Equipe de Tratamento e Resposta a Incidentes à Segurança das Informações (ETRISI);

V. Coordenar o Comitê de Segurança da Informação e Comunicações (CSIC);

VI. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicações;