INSTITUTO FEDERAL
Alagoas

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE ALAGOAS
CONSELHO SUPERIOR/IFAL

RESOLUÇÃO Nº 111 / 2023 - CONSUP/IFAL (11.20)

Nº do Protocolo: 23041.014905/2023-81

Maceió-AL, 25 de abril de 2023.

Aprova, ad referendum do Conselho Superior, a Política de Segurança da Informação no âmbito do Instituto Federal de Alagoas - Ifal.

O PRESIDENTE DO CONSELHO SUPERIOR do Instituto Federal de Alagoas - IFAL, órgão de caráter consultivo e deliberativo da Administração Superior, no uso de suas atribuições conferidas pelo § 3º do Art. 10 da Lei nº 11.892, de 29/12/2008, publicada no DOU de 30/12/2008, nomeado pelo Decreto Presidencial de 10/6/2019, publicado no DOU nº 111, Seção 02, de 11/6/2019 e em conformidade com o Estatuto da Instituição.

Considerando o Processo nº 23041.026701/2021-21, de 19/8/2021.

Considerando o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, disponível em: **http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm**.

Considerando o Decreto nº 10.641, de 02 de março de 2021, que altera o Decreto nº 9.637, **disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm.**

Considerando a Instrução normativa 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, disponível em: **https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215.**

Considerando a Resolução nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor da Segurança da Informação, disponível em **https://www.in.gov.br/en/web/dou/-/resolucao-n-1-de-11-de-setembro-de-2019-217042776.**

Considerando o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética, disponível em **http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm**.

Considerando a Portaria nº 93, de 26 de setembro de 2019, que aprova o Glossário de **Segurança da Informação, disponível em https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1.**

RESOLVE

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito do Instituto Federal de Alagoas - Ifal.

CAPÍTULO I - ESCOPO

Art. 2º A Política de Segurança da Informação do Ifal institui normas, diretrizes e princípios de segurança da informação, que devem ser cumpridas por todos servidores, usuários e prestadores de serviços, com intuito de assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação do Ifal.

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Art. 3º Conceitos e definições abordadas na Política de Segurança da Informação do Ifal, são tratados e atualizados no Glossário de Segurança da Informação, instituído pelo Gabinete de Segurança Institucional da Presidência da República. O Glossário de Segurança da Informação constante na Portaria nº 93, de 26 de setembro de 2019, da Presidência da República/Gabinete de Segurança Institucional.

CAPÍTULO III - ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 4º A estrutura de gestão de Segurança da Informação compreende:

a. Gestor de Segurança da Informação;

b. Comitê de Segurança da Informação; e

c. Equipe de Tratamento e Resposta a Incidentes de Segurança.

CAPÍTULO IV - PRINCÍPIOS

Art. 5º As normas e diretrizes da Política de Segurança da Informação do Ifal deverá se guiar pelos seguintes princípios:

I. não repúdio: os sistemas devem garantir que um indivíduo que realizou ação não possa negar a sua autoria. Isso se aplica, por exemplo, ao envio de e-mails e à realização de transações em sistemas de informação;

II. menor privilégio: usuários de sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para o exercício de suas funções;

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

IV. auditabilidade: todos os eventos significativos de sistemas e processos devem ser rastreáveis até o evento inicial;

V. mínima dependência de segredos: os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam;

VI. controles automáticos: Sempre que possível, controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano;

VII. resiliência: os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre e retornar à normalidade das operações;

VIII. -defesa em profundidade: Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada

para prevenir a brecha de segurança;

IX. exceção aprovada: Exceções a esta política deverão sempre ter aprovação do Comitê de Segurança de Informação do Ifal;.

X. substituição da segurança em situações de emergência: Controles somente devem ser desconsiderados de formas pré determinadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência; e

XI. esta política deve estar também em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como aos demais dispositivos legais aplicáveis.

CAPÍTULO V - DIRETRIZES GERAIS

Art. 6º São diretrizes gerais desta política:

I. as diretrizes de segurança da informação devem considerar, prioritariamente, as normas e os objetivos estratégicos definidos nos decretos e portarias que norteiam a Política Nacional de Segurança da Informação;

II. as diretrizes de segurança da informação devem considerar, também, as normas da Associação Brasileira de Normas Técnicas (ABNT) relacionadas à Segurança da Informação;

III. os custos associados à gestão de segurança da informação deverão ser compatíveis com os custos dos ativos que se deseja proteger;

IV. a gestão de segurança da informação deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos da Política Nacional de Segurança da Informação; e

V. as normas e procedimentos de segurança da informação devem considerar, subsidiariamente, normas e padrões aceitos no mercado.

Art. 7º São diretrizes específicas desta política, que serão detalhadas em normatização própria:

I. tratamento da informação;

II. segurança física e do ambiente;

III. gestão de incidentes em segurança da informação;

IV - gestão de ativos;

IV. gestão do uso dos recursos operacionais e de meios de comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;

VI. controles de acesso;

VII - gestão de riscos;

VIII. gestão de continuidade; e

IX - auditoria e conformidade.

CAPÍTULO VI - COMPETÊNCIAS

Art. 8º São competências dos gestores e de todos que têm acesso dos ativos do IFAL:

I. é de responsabilidade da alta administração do Ifal prover a orientação e o apoio necessários às ações de gestão da segurança da informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes;

II. é de responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes desta política no âmbito de suas áreas de atuação; e

III. é de responsabilidade de todos que têm acesso aos ativos do IFAL manter níveis de segurança da informação adequados, segundo preceitos desta política e de suas normas complementares.

CAPÍTULO VII - PENALIDADES

Art. 9º Ações que violem a Política de Segurança da Informação-Ifal ou suas normas, que quebrem os controles de segurança da informação e comunicações, ou que tenham o potencial de causar danos aos ativos do Ifal serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Parágrafo único. Processo disciplinar específico deverá ser elaborado para apurar as ações que constituem a quebra das diretrizes impostas por esta política de segurança da informação.

CAPÍTULO VIII - POLÍTICA DE ATUALIZAÇÃO

Art. 10 Esta política deve ser atualizada a cada 02 (dois) anos pelos integrantes do Comitê de Segurança da Informação do Ifal, ou antes, em casos excepcionais.

Art. 11 Esta Resolução entrará em vigor na data da sua publicação.

(Assinado digitalmente em 25/04/2023 11:11)
CARLOS GUEDES DE LACERDA
REITOR - TITULAR
REIT (11.01)
Matrícula: 1085939

Para verificar a autenticidade deste documento entre em **https://sipac.ifal.edu.br/public/documentos/index.jsp** informando seu número: **111**, ano: **2023**, tipo: **RESOLUÇÃO**, data de emissão: **25/04/2023** e o código de verificação: **77e9c0f4d3**