



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

DELIBERAÇÃO CGSIC/ IFS Nº 10, DE 29 DE SETEMBRO DE 2023

Aprova a Política de Gestão de Ativos de Informação do Instituto Federal de Sergipe - IFS.

A PRESIDENTE DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008 e o Art. 11 do Estatuto do IFS, em conformidade com as Portarias IFS nº 1.039 de 28/04/2014, 1.339 de 05/06/2014 e 3.795 DE 06/12/2019, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e considerando a 3ª reunião ordinária do Comitê Gestor de Segurança da Informação e Comunicação em 2023, ocorrida em 25/09/2023,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Aprovar a Política de Gestão de Ativos de Informação do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS, com o objetivo de definir princípios, diretrizes, objetivos, normas, responsabilidades, condições e precauções em relação à gestão de ativos de Informação, no âmbito do IFS, a fim de garantir o nível de segurança da informação assegurando que os ativos de informação sejam identificados adequadamente, e que os controles de proteção recomendados/determinados pela legislação competente para a privacidade e proteção dos dados nestes ativos estejam em vigor.

Art. 2º Para manter a segurança e continuidade do negócio do IFS, em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de riscos da organização, além de auxiliar na recuperação de incidentes.

Art. 3º Os ativos de informação do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe IFS devem ser classificados a fim de permitir a definição de seus níveis de segurança. Cada ativo de informação deverá ter um proprietário, que deverá classificá-lo e registrá-lo em uma base de dados gerenciada de forma centralizada.

Art. 4º A Política de Gestão de Ativos de informação está alinhada com as Políticas de Segurança da Informação (POSIC), Gestão de Riscos e Controle Internos (PGRC) e de Gestão de Continuidade de Negócios (PGCN) do IFS.



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

Seção I
Do Escopo

Art. 5º Esta política se aplica a todos os ativos de informação do IFS, incluindo ativos fora dos domínios físicos da instituição, por exemplo dados armazenados em um serviço de nuvem.

§1º Ativos de informação neste contexto, incluem documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mails, arquivos pessoais e compartilhados, bancos de dados e conteúdos específicos da web.

§ 2º A classificação dos ativos de informação e o escopo desta política devem ser revisados periodicamente.

Seção II
Das definições

Art. 6º A presente deliberação considera as definições do Glossário de Segurança da Informação, definido na Portaria PR/GSI nº 93, de 18 de outubro de 2021, adaptado ao contexto do IFS nas seguintes definições:

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

II - TI: sigla de tecnologia da informação;

III - Ativo de tecnologia da informação – ativo de TI: meio tecnológico de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso e sistemas utilizados para tal;

IV - Ativo de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, ativos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

V - DTI: Diretoria de Tecnologia da Informação do IFS;

VI - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

VII - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

VIII - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIX - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa natural, ou por um determinado sistema, órgão ou entidade;

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

XI - Ameaça: conjunto de fatores com o potencial de causarem dano para um sistema ou organização;

XII - Incidente de segurança da informação: evento que comprometa ou tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

XIII - Medida técnica: controle relacionado à segurança cibernética, obtido por processo que possibilite confidencialidade, disponibilidade e integridade dos dados e conformidade legal e normativa;

XIV - Medida administrativa: controle organizacional, físico ou procedimental, obtido por processo que possibilite, confidencialidade, disponibilidade e integridade dos dados e conformidade legal e normativa; e

XV - Tratamento: toda operação realizada com dados e informações, como as que se referem à coleta, produção, recepção, avaliação ou controle da informação, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência, difusão ou extração.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 7º A concepção, desenvolvimento e operação dos ativos de TI do IFS devem ser realizados atendendo a boa-fé e respeitando os seguintes princípios:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades e objetivos, de acordo com o contexto do tratamento;

III - Necessidade: limitação das ações do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades e objetivos; do tratamento de dados;

IV - Segurança: utilização de medidas técnicas e administrativas aptas a proteger de acessos não autorizados os ativos de informação e dados. Seja em situações acidentais ou ilícitas de destruição,



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

perda, alteração e comunicação ou difusão não autorizada por legislação ou por ordem judicial, durante o processo de tratamento;

V - Prevenção: adoção de medidas para prevenir a ocorrência de danos decorrentes do processo de tratamento de dados;

VI - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

VII - Legalidade: utilização lícita de ativos de TI para finalidades relacionadas ao vínculo do usuário com o IFS;

VIII - Economicidade: utilização de ativos de TI para obtenção do resultado esperado com o menor custo possível, com precaução, celeridade e qualidade na prestação do serviço ou no trato com os bens públicos.

Art. 8º As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação do IFS, a fim de manter o escopo da organização mapeado e documentado.

CAPÍTULO III
DAS DIRETRIZES

Art. 9º A implementação da gestão de ativos de informação observará as seguintes diretrizes:

I - Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado;

II - A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização;

III - A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software;

IV - A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor;

V - A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos;

VI - A organização utilizará ferramentas de inventário de software, quando possível, para automatizar a descoberta e documentação dos softwares instalados;

VII - A organização assegurará que exista um processo semanal para lidar com ativos não autorizados;



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

VIII - A organização utilizará controles técnicos em todos os ativos para garantir que apenas softwares autorizados sejam executados, sendo estes reavaliados semestralmente ou com mais frequência;

IX - A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados e assinados digitalmente tenham permissão para serem executados;

X - A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: Dynamic Host Configuration Protocol (DHCP) - para atualizar o inventário de ativos da instituição;

XI - O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação;

XII - As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação;

XIII - Cada ativo de informação (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, deve ter uma etiqueta afixada ao dispositivo para fins de identificação;

XIX - Deverá ser registrado no identificador de ativos da informação outras informações relevantes no inventário de TI:

- a) Identificador de ativos,
- b) Data da compra,
- c) Preço de compra,
- d) Descrição do item,
- e) Fabricante,
- f) Número do modelo,
- g) Número de série,
- h) Nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável,
- i) Localização física do ativo da empresa, quando aplicável,
- j) Endereço físico (controle de acesso à mídia (MAC))
- k) Endereço de Protocolo de Internet (IP),
- l) Data de validade da garantia/vida útil,
- m) Qualquer informação de licenciamento relevante,
- n) No caso de softwares instalados na organização deve ser registrado no inventário informações como:
 - Título do software,
 - Desenvolvedor ou editor de software,



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

- Data de aquisição,
- Data de instalação,
- Duração do uso,
- Finalidade comercial,
- Lojas de aplicativos;
- Versões,
- Mecanismo de implantação,
- Data de fim do suporte, se conhecida,
- Qualquer informação de licenciamento relevante,
- Data de descomissionamento.

CAPÍTULO IV

DO PROCESSO DE MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 10. O processo de mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 11. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos do IFS, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art. 12. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:

- I - Os responsáveis (proprietários e custodiantes) de cada ativo de informação;
- II - As informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;
- III - Os contêineres de cada ativo de informação; e
- IV - As interfaces de cada ativo de informação e as interdependências entre eles.

Parágrafo único. O registro de ativos de informação deverá ser realizado pelo Responsável Técnico de TI e homologado pelo Responsável Administrativo de TI em sistema disponibilizado pelo DTI.

Art. 13. Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

- a) Ativos físicos;



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

- b) Bancos de dados;
- c) Dispositivos móveis;
- d) Hardwares;
- e) Mídias removíveis;
- f) Níveis de permissões;
- g) Serviços;
- h) Softwares.

Art. 14. Os ativos TIC são divididos em ativos de hardware, de software e de dados:

I. São considerados ativos de hardware: equipamentos de escritório, como: computadores de mesa e portáteis, monitores, nobreaks, impressoras, telefones VOIP, etc; de infraestrutura, como: servidores, switches, roteadores, etc;

II. São considerados ativos de software: aplicações desenvolvidas pelo IFS, aplicações desenvolvidas por outros órgãos públicos e hospedadas no IFS, aplicações de software livre e licenças de aplicações de terceiros adquiridas; e

III. São considerados ativos de dados: dados armazenados em sistemas de informação no formato lógico, elétrico, magnético, óptico, físico, ou impresso, que podem ainda ser classificados como dados pessoais, de interesse e propriedade do usuário, ou dados corporativos, de interesse e propriedade ou sob a guarda do IFS.

Seção I

Da gestão e monitoramento de Ativos de Informação

Art. 15. Os ativos de TI devem ser monitorados para garantir seu funcionamento adequado e fornecer informações para o gerenciamento de capacidade e demanda, para remanejamento e descarte.

§1º O remanejamento de ativos de TI deve ser priorizado em detrimento do descarte.

§2º Todos os ativos de TI com armazenamento de dados deverão ser analisados criticamente antes de serem enviados para manutenção, serem descartados, doados, remanejados ou reutilizados, com a finalidade de assegurar a proteção e confidencialidade das informações existentes.

§3º Ao fim do seu ciclo de vida útil, a informação e seu meio de armazenamento, quando aplicável, deverá ser descartada de forma segura, compatível com a sua classificação de segurança.

§4º Os investimentos em TI devem priorizar infraestruturas compartilhadas, visando atender ao maior número de usuários possível.



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

§5º O planejamento da aquisição e gestão dos ativos de TI deve estar alinhado com o PDTIC vigente.

Art. 16. Cabe ao responsável pela gestão dos ativos de informação:

- I - identificar e classificar os ativos de informação por nível de criticidade;
- II - identificar potenciais ameaças aos ativos de informação;
- III - identificar vulnerabilidades dos ativos de informação;
- IV - consolidar em um relatório informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação;
- V - autorizar a atualização do relatório mencionado no inciso IV do caput;
- VI - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação; e
- VII - Implementar mecanismos de segurança adequados, visando reduzir os riscos identificados.

Seção II

Dos Papeis e Responsabilidades

Art. 15. A Coordenadoria de Tecnologia da Informação - CTI, na figura do coordenador, responsável administrativo de TI, será o ponto de contato da Unidade com a Diretoria de Tecnologia da Informação para tratar das questões de TI, e receber comunicações de interesse da Unidade.

§1º O Responsável Administrativo de TI deve ser um servidor de TI do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe.

§2º São responsabilidades do Responsável Administrativo de TI:

- I - Ser o contato oficial da unidade ou órgão com o DTI para assuntos relacionados à infraestrutura e serviços de TI;
- II - Conhecer o catálogo de serviços do IFS;
- III - Participar da Equipe de Tratamento de Incidentes de TI do IFS;
- IV - Orientar os usuários da unidade ou órgão em relação à:
 - a) Limites de atuação da estrutura de suporte de TI da própria Unidade, caso existente;
 - b) Necessidade de planejamento para alterações na infraestrutura de TI;
 - c) Abertura de chamados na Central de Serviços de TI do IFS;
- V - Divulgar internamente as informações relativas à TI no IFS;
- VI - Nomear e manter atualizada a lista dos Responsáveis Técnicos de TI da unidade ou órgão.



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

§3º As unidades do IFS podem ter um ou mais Responsáveis Técnicos de TI, apontados pelo Responsável Administrativo de TI.

§4º O Responsável Administrativo de TI pode acumular o papel de Responsável Técnico de TI.

§5º São responsabilidades do Responsável Técnico de TI:

I - Apoio na instalação e configuração de softwares e serviços de TI do IFS;

II - Apoio nas atividades relativas à infraestrutura física de rede da Unidade;

III - Apoio no suporte à rede e dispositivos de rede da Unidade;

IV - Apoio na configuração e manutenção de servidores, computadores e outros dispositivos de TI da Unidade;

V - Apoio na prevenção e no tratamento de incidentes de segurança da informação;e

VI - Registro de ativos de informação em sistema disponibilizado pela DTI.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 16. Todas as redes de dados do IFS deverão seguir os padrões mínimos operacionais e de segurança definidos pela Coordenadoria de Segurança da Informação - COSEG.

§1º É vedada a instalação de equipamentos na rede do IFS, como switches, roteadores, pontos de acesso sem fio (APs), ou quaisquer equipamentos que possam interferir nos sistemas de informação ou no tráfego de dados na rede, sem a devida homologação da COSEG e autorização da CTI da Unidade.

§ 2º É vedada a instalação de ativos de TI que não atendam aos padrões operacionais e de segurança definidos ou que visem alterar ou evitar os mecanismos de segurança existentes nos sistemas ou na infraestrutura de rede.

Art. 17. O ambiente físico dos ativos de TI deve ser adequado aos requisitos técnicos do ativo e ter a segurança física adequada ao valor do respectivo ativo de informação e aos riscos identificados.

Art. 18. Violações desta política poderão resultar na suspensão, bloqueio ou restrição de acesso aos ativos de TI do IFS, de forma temporária ou permanente, sem prejuízo à aplicação de sanções administrativas, penais e cíveis.

Art. 19. A gestão de ativos de TI que origine incidente de segurança ou violação a determinações legais estão sujeitos às sanções previstas na legislação competente.

Parágrafo único A ausência de providências ou a não observância das determinações legais pode acarretar repercussões negativas ao IFS e em sanções administrativas, civis e penais, isolada ou cumulativamente, aos responsáveis, nos termos da legislação aplicável, assegurado aos envolvidos o contraditório e a ampla defesa.



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

Art. 20. A política de gestão de ativos de informação deve estar disponível no endereço (<https://www.ifs.edu.br/politica-de-seguranca-da-informacao-e-comunicacao.html>).

Art. 21. Esta política poderá ser desdobrada em outros documentos normativos específicos, que deverão preservar coerência e alinhamento com os elementos norteadores nesta estabelecidos.

Art. 22. A política será revisada anualmente, quando surgirem novos requisitos corporativos, alterações na legislação competente ou conforme necessidade do CGSIC.

Art. 23. Os casos omissos e as situações imprevistas serão encaminhados à avaliação e decisão da autoridade máxima do IFS.

Art. 24. A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.

Art. 25. Esta política entra em vigor no dia 1º de outubro de 2023, em conformidade com o disposto no art. 4º, parágrafo único, do Decreto nº 10.139, de 28 de novembro de 2019.

Aracaju, 29 de setembro de 2023.

Ruth Sales Gama de Andrade

Presidente do CGSIC/IFS