Ministério da Educação
INSTITUTO FEDERAL DO ACRE

RESOLUÇÃO CONSU/IFAC Nº 242, DE 09 DE SETEMBRO DE 2025

Dispõe sobre a aprovação da Política de Gestão de Ativos do Instituto Federal de Educação, Ciência e Tecnologia do Acre.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO ACRE (IFAC), no uso de suas atribuições legais conferidas pelo artigo 12 da Lei nº 11.892, de 29 de dezembro de 2008, nomeado pelo Decreto Presidencial de 30 de setembro de 2024, publicado no Diário Oficial da União – DOU nº 190, seção 2, página 1, de 1º de outubro de 2024,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução estabelece:

I - Aprovar a Política de Gestão de Ativos do Instituto Federal de Educação, Ciência e Tecnologia do Acre (Ifac).

Meta

II - assegurar a identificação e a classificação dos ativos da informação pertencentes ao Ifac, bem como visa garantir a implementação e a manutenção de controles de proteção adequados à criticidade e ao valor estratégico de cada ativo, em consonância com as melhores práticas e regulamentações aplicáveis. As diretrizes impostas neste documento têm como objetivo melhorar a segurança e garantir a continuidade do negócio do Ifac e, para isso, o mapeamento e monitoramento dos ativos tecnológicos são fundamentais, visto o auxílio na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização.

Escopo

III - esta Política se aplica a todos os ativos de informação, dos quais o Ifac seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento. Especificamente, inclui:

a) Todos os funcionários, sejam servidores efetivos ou temporários, do Ifac;

b) Todos os contratados e terceiros que trabalham para o Ifac;

c) Todos os funcionários de parceiros que acessam a rede e sistemas de informação do Ifac; e

d) Todos os alunos, bolsistas, menores aprendizes e estagiários;

Objetivos

IV - este documento tem como objetivos:

a) Eficiência e Sustentabilidade: Estabelecer diretrizes para o gerenciamento eficiente e sustentável dos ativos do Ifac. Isso inclui otimizar o uso dos recursos, prolongar a vida útil dos ativos, minimizar custos operacionais e de manutenção, e garantir a conformidade com as regulamentações aplicáveis, contribuindo para um ambiente de aprendizado de qualidade e a sustentabilidade financeira da instituição;

b) Qualidade do Ambiente de Aprendizagem e Segurança: Garantir que os ativos do Ifac sejam gerenciados de forma a apoiar a qualidade do ambiente de aprendizado, a segurança de todos os usuários e a continuidade das operações. Isso envolve a manutenção adequada dos equipamentos e instalações, a atualização tecnológica quando necessário, a prevenção de perdas e danos, e a garantia de um ambiente seguro e funcional para estudantes, professores e servidores;

c) Transparência e Responsabilidade: Estabelecer um sistema de gestão de ativos transparente e com responsabilidades claramente definidas em todos os níveis do Ifac. Isso envolve a criação controles claros para o registro, utilização, manutenção e descarte de ativos, a designação de responsáveis por cada etapa do ciclo de vida dos ativos, e promoção de uma cultura de responsabilidade e prestação de contas em relação ao patrimônio da Instituição.

Termos e Definições

Aplicação: programa de computador hospedado em ambientes de datacenter (ativos de infraestrutura).

Ativo: aquilo que tem valor – tangível ou intangível - para a organização (tais como informação, *software*, equipamentos, instalações, serviços, pessoas e imagem institucional).

Ativo Crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização.

CORTI: acrônimo para Coordenação de Tecnologia da Informação (TI).

Endereço MAC (MAC Address): endereço físico da interface de um dispositivo de rede, utilizado para transporte na camada 2 (Enlace) do Modelo OSI.

ETIR: acrônimo para Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

Hardware: parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam por meio de barramentos.

Hypertext Transfer Protocol Secure (HTTPS): extensão do HTTP utilizada para comunicação segura pela rede de computadores. No HTTPS, o protocolo de comunicação é criptografado usando o TLS ou o seu predecessor, o SSL. A principal motivação para o uso do HTTPS é a autenticação do site acessado e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações.

Internet Protocol (IP): endereço IP, de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP (Internet Protocol ou Protocolo de internet) único, que é o meio em que as máquinas usam para se comunicarem na Internet.

Patch: atualizações de sistemas.

Software: programa de computador utilizado em estações de trabalhos (ativos de usuário final).

SSH: Secure Shell. Protocolo que fornece uma maneira segura de acessar e gerenciar sistemas remotamente.

Referência Legal e Boas Práticas

Orientação	Secção
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Guia do Framework de Privacidade e Segurança da Informação	Controles 1, 2 e 12
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Instrução Normativa Nº 05/GSI/PR, de 30 de agosto de 2021	Anexo
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta	
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Enterprise Asset Management Policy Template CIS v8	Em sua íntegra
Software Asset Management Policy Template CIS v8 - Novembro de 2022	Em sua íntegra

CAPÍTULO II

RESPONSABILIDADE E ATRIBUIÇÕES

Art. 2º O Ifac deverá inventariar os ativos internos – *hardware*, *software* e aplicações – capazes de armazenar ou processar dados, conforme o escopo estabelecido.

Art. 3º Durante o registro de ativos de *hardware* deverão ser consideradas informações, incluindo, mas não se limitando a:

I - endereço de rede (IP);

III - endereço de *hardware* (MAC Address);

III - nome da máquina;

IV - coordenação responsável;

V - autorização para se conectar à rede; e

VI - sistema operacional.

Art. 4º Durante o registro de ativos de *software* deverão ser consideradas informações, incluindo, mas não se limitando a:

I - título do *software*;

II - desenvolvedor ou fabricante de *software*;

III - data de aquisição;

IV - data de instalação;

V - versão; e

VI - data de fim de suporte, quando aplicável.

Art. 5º Durante o registro de aplicações deverão ser consideradas informações, incluindo, mas não se limitando a:

I - link de acesso;

II - descrição;

III - máquinas virtuais e serviços relacionados;

IV - containers envolvidos, quando aplicável;

V - logs de acesso;

VI - logs de aplicação;

VII - localização dos arquivos relacionados à aplicação, quando aplicável; e

VIII - linguagens e tecnologias utilizadas.

Art. 6º A identificação dos ativos críticos de *hardware*, *software* e dispositivos de rede deverá ser considerada como prioridade.

Art. 7º Os ativos não autorizados no ambiente do Ifac deverão ser identificados e, posteriormente, removidos ou impedidos de acessar a rede.

Art. 8º Sempre que possível, deverão ser utilizadas ferramentas de descoberta ativa para identificar os ativos conectados à rede.

Art. 9º O Ifac deve assegurar que apenas *softwares* com suporte ativo dos seus desenvolvedores sejam utilizados em seu ambiente.

Art. 10. *Softwares* sem suporte ativo e que não recebem atualizações ou *patches* de segurança deverão ser identificados e classificados como exceções, para que seus riscos sejam avaliados e ações de mitigação sejam implementadas.

Art. 11. Aplicações desenvolvidas internamente deverão ser inventariadas junto aos demais ativos do Ifac, apontando também o proprietário e responsável.

Art. 12. Aplicações desenvolvidas e identificadas internamente que apresentarem riscos de segurança significativos ao Ifac poderão ser desativadas temporariamente e avaliadas pela ETIR.

Art. 13. O inventário de ativos críticos deve ser revisado e atualizado semestralmente, levando em consideração as alterações nos ativos de informação do Ifac.

Art. 14. O inventário de ativos deve ser revisado e atualizado anualmente, considerando as alterações nos ativos de informação do Ifac.

Art. 15. O Ifac deverá assegurar que a infraestrutura de rede da instituição seja atualizada semestralmente, utilizando versões estáveis e com correções aplicadas para vulnerabilidades conhecidas.

Art. 16. Em casos de sistemas ou componentes obsoletos na infraestrutura de rede essenciais para o funcionamento do Ifac, estes deverão ser identificados, junto aos seus riscos, e ações de mitigação deverão ser implementadas.

Art. 17. O gerenciamento de redes deverá ser realizado por meio de protocolos de rede seguros, como SSH e HTTPS.

Art. 18. O Ifac deverá estabelecer um diagrama de arquitetura de rede de forma que seja representada visualmente as atividades e componentes da rede interna.

CAPÍTULO III

PAPÉIS E RESPONSABILIDADES

Art. 19. Caberá à alta gestão do Ifac:

I - promover e apoiar o cumprimento das diretrizes dispostas nesta política;

II - apoiar as áreas relacionadas para o cumprimento das diretrizes desta política; e

III - destinar recursos para a execução das diretrizes desta política.

Art. 20. Caberá à Coordenação de Segurança da Informação:

I - coletar informações acerca dos ativos de rede encontrados no instituto utilizando, quando possível, meios automatizados;

II - operacionalizar as diretrizes e controles descritos nesta política;

III - trabalhar em conjunto com as áreas relacionadas para o cumprimento das normas e diretrizes dispostas nesta política; e

IV - identificar na rede ativos que não foram previamente autorizados e realizar a negação de suas conexões de acordo com procedimento próprio.

Art. 21. Caberá à Coordenação de Suporte:

I - operacionalizar as diretrizes e controles descritos nesta política no escopo dos dispositivos de usuários finais e impressoras da Reitoria;

II - trabalhar em conjunto com as áreas relacionadas para o cumprimento das normas e diretrizes dispostas nesta política;

III - avaliar os ativos cedidos para atividades laborais em toda a instituição; e

IV - avaliar e aprovar atualizações e novas versões de *softwares* nos ativos de informação anteriormente citados.

Art. 22. Caberá à Coordenação de Sistemas:

I - fornecer as informações relevantes das aplicações desenvolvidas internamente para identificação no inventário de TI;

II - operacionalizar as diretrizes e controles descritos nesta política no escopo dos sistemas implantados e desenvolvidos pela coordenação;

III - trabalhar em conjunto com as áreas relacionadas para o cumprimento das normas e diretrizes dispostas nesta política; e

IV - avaliar e aprovar atualizações e novas versões de *softwares* nos ativos de informação.

Art. 23. Caberá à CORTI dos *campi*:

I - operacionalizar as diretrizes e controles descritos nesta política conforme previsto no art. 2º;

II - trabalhar em conjunto com as áreas relacionadas para o cumprimento das normas e diretrizes dispostas nesta política; e

III - operacionalizar atualizações e novas versões de *softwares* nos ativos de informação.

Art. 24. Caberá aos usuários:

I - seguir as diretrizes e controles descritos nesta política; e

II - realizar a devolução dos ativos de informação após a rescisão do contrato de trabalho ou outro tipo de contrato, quando aplicável.

CAPÍTULO IV

CLASSIFICAÇÃO DO NÍVEL DE ACESSO ÀS INFORMAÇÕES

Art. 25. Todos os ativos de informação deverão ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso a informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), e demais normas aplicáveis.

Art. 26. As informações armazenadas, transmitidas, processadas ou que se encontram sob a custódia dos ativos de informação do Ifac, independentemente de seu formato e suporte, deverão ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.

Art. 27. A classificação de nível de acesso das informações deverá observar as diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012, e outros normativos complementares que abordam o assunto.

Art. 28. As informações deverão ser classificadas conforme os seguintes níveis de acesso:

I - pública, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

II - restrita, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e

III - sigilosa, classificada em grau de sigilo, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

Art. 29. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela Instituição.

CAPÍTULO V

USO ACEITÁVEL

Art. 30. Os padrões ou diretrizes para o uso aceitável de ativos deverão ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

Art. 31. Os seguintes itens deverão ser cobertos nas diretrizes de uso aceitáveis:

I - uso do computador e dos sistemas de informação;

II - uso de *softwares* e dados;

III - uso da Internet e *e-mail*; e

IV - uso de equipamentos e materiais de escritório.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 32. Esta Resolução entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Fábio Storch de Oliveira**, **Presidente**, em 09/09/2025, às 16:53, conforme horário oficial de Rio Branco (UTC-5), com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifac.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1201950** e o código CRC **6490D4E2**.
