

RELATÓRIO DE GESTÃO

2025



Janeiro
2026



UFAM

1. Quais as principais ações executadas pelo CTIC?

Em 2025, o Centro de Tecnologia da Informação e Comunicação (CTIC) executou modernizações significativas e o desenvolvimento de novas soluções para os sistemas da instituição. Além disso, diversas atividades estenderam-se às demais áreas de atuação do Centro, com ênfase em:

- Expansão e manutenção de serviços de infraestrutura de rede;
- Serviços de atendimento ao usuário;
- Gestão de contratos de TIC e apoio à aquisição de recursos;
- Levantamento de artefatos para registro de preços;
- Elaboração e deliberação de políticas institucionais de TIC.

Entre as principais ações monitoradas, gerenciadas ou executadas no âmbito de sistemas institucionais, destacam-se os indicadores abaixo dos principais sistemas institucionais gerenciados pelo CTIC:

ECampus – Principal sistema acadêmico/administrativo mantido pelo CTIC:

- Implementação do módulo de Termos de Compromisso de Estágio: integração com o novo assinador digital da UFAM, totalizando 3.268 termos assinados em 2025;
- Matrículas: 338 mil solicitações (crescimento de 7,8% em relação a 2024), com 168 mil matrículas efetivadas após o processamento;
- Documentação: 823.936 documentos autenticados gerados, destacando-se:
 - 278 mil históricos escolares analíticos;
 - 5.249 certidões de "nada consta";
 - 3.600 certificados de projetos;
- Projetos: 3 mil submissões de projetos de pesquisa, inovação e extensão.

SAUIM (Sistema Acadêmico Unificado de Informação e Monitoramento da UFAM):

- Implementação de Inteligência Artificial (IA) para monitoramento acadêmico avançado;
- Predição de evasão estudantil com explicabilidade dos fatores determinantes via IA.

PSConcursos – Sistema eletrônico de processos seletivos:

- Implantação de módulos específicos para ingresso de refugiados (PSRefugiados) e aperfeiçoamento do sistema para ingressantes de Música (PSMúsica).

SisRU (Sistema de Restaurante Universitário):

- **Gestão de Consumo:** Registro sistemático de mais de 750 mil refeições (café, almoço e jantar) em todos os campi da UFAM (capital e interior);
- **Sistema de Canecas Sustentáveis:** Módulo integrado ao SisRU para controle de distribuição; foram disponibilizadas mais de 3.700 canecas para discentes com frequência comprovada no RU em 2025.

RU Digital – Sistema de venda de tickets virtuais:

- 63 mil visualizações de página;
- 2 mil links de pagamento gerados;
- 6 mil refeições vendidas desde a implementação (novembro de 2025).

Ademais, em relação a serviços de manutenção de sistemas, registrados no GLPI em 2025, foram **1514 (dos quais 1426, 94%, foram fechados/solucionados) chamados** relacionados à manutenção de sistemas, relatórios de sistemas ou mudanças e melhorias de funcionalidades nos sistemas.

Destacam-se também, no âmbito de políticas institucionais de TIC, a deliberação e publicação da Política de Controle de Acesso a Recursos de TIC, cuja relatoria original é deste Centro e com impacto direto na geração de planos de ação para melhor controle de acesso a sistemas e recursos computacionais — entre eles, a deliberação da autenticação multifatores (MFA) no e-mail institucional da UFAM, com ampla divulgação institucional em 2025. Além dela, foi deliberada e discutida a Política de uso do Google Workspace, com decisão posterior, no CONSAD, de conversão para Portaria, a ser lançada em 2026.

Ainda relacionado à questões de segurança da informação, destaca-se que a instituição avançou no **ciclo 5 do PPSI** (Programa Permanente de Segurança da Informação), estabeleceu a **Equipe de Tratamento de Incidentes de Rede (ETIR)** e tratou **59 incidentes de segurança**. Também foram realizadas campanhas de conscientização sobre phishing, engenharia social e proteção de dados sensíveis, detalhados no item 8 do presente relatório.

No âmbito da infraestrutura de rede e atendimento institucional, destaca-se a criação de 38 portais institucionais em 2025, a intermediação de 22 mil acessos a recursos de TIC via CAFé UFAM, 4 mil chamados criados no portal de serviços de TIC da UFAM (o suporte CTIC), com um índice de conclusão de 94%. Além disso, o CTIC destaca que foram implantados mais de 500 pontos de rede distribuídos em diversas unidades acadêmicas, incluindo FT, ICE, FES, IEAA, FACED, FCA, FEFF, Odontologia, Medicina e Enfermagem. Realizadas instalações de 15 patch panels, 3 racks, além de 684 metros de cabos ópticos com 6 conectorizações e fusões de fibra óptica. A expansão cobriu laboratórios, setores administrativos, sistema de câmeras de segurança e pontos WiFi.

Em relação às ações de planejamento e contratações de TIC geridas pelo CTIC, foram renovados 9 contratos estratégicos totalizando mais de R\$ 4 milhões em dotação planejada, abrangendo redes ópticas, VPN NGFW, sistema SIE, suporte a equipamentos do datacenter, computação em nuvem e telefonia institucional. Novas contratações incluíram licença Veeam para backup de dados (R\$ 62,7 mil) e Google Workspace Education Plus (R\$ 375,4 mil), no qual o CTIC atua como parceiro em conjunto com a PROEG.

Em relação aos atendimentos aos usuários, através de suporte técnico, o serviço de suporte registrou **1.849 chamados atendidos via GLPI (Suporte CTIC) com taxa de resolução de 99,5%**. Os principais serviços foram relacionados a equipamentos de TIC (25%), sistemas institucionais (24%), recursos de TIC (8%) e gestão de e-mail (15%). O tempo médio de resolução foi de 3,1 dias, conforme dados do GLPI.

2. Quais os principais desafios futuros do CTIC em relação à tecnologia da informação na UFAM?

Os desafios futuros do CTIC, sobretudo em 2026, estruturam-se em torno de quatro eixos principais: i) modernização da infraestrutura crítica, ii) adequação de sistemas legados, iii) expansão da segurança da informação e iv) atualização e conformidade com o recém aprovado Plano de Desenvolvimento Institucional (PDI) 2026-2030.

Eixo 1: Modernização da Infraestrutura Crítica

Renovação do Firewall Institucional (Palo Alto) representa um dos desafios mais urgentes para 2026, com investimento estimado entre R\$ 2,5 e 3,3 milhões (a depender da duração do contrato). O equipamento atual terá seu fim de vida útil e encerramento do contrato de suporte previstos para 2026, representando impacto crítico à segurança da instituição. Sem a atualização, a UFAM ficaria vulnerável a ataques externos por falta de proteção moderna, além de comprometimento do roteamento de tráfego interno e externo e riscos à gestão de configuração de domínio, entre outras operacionalizações de redes e segurança da informação.

Aquisição de Switches Core, necessária para ampliação da capacidade da rede principal, além da substituição do equipamento switch core vigente, defasado e com problemas no suporte a capacidade de rede atual da UFAM. A modalidade de aquisição prevista é Sistema de Registro de Preços (SRP), visando viabilizar a expansão de banda para novos serviços e suportar o crescimento da demanda institucional.

Expansão de Cobertura WiFi visa atender a meta do PDI 2026-2030 (M5 - OE11.1) de prover infraestrutura em 100% das unidades até 2030. Será necessária a aquisição de Access Points (APs) através de SRP para prover a expansão da rede WiFi, atualmente limitada pela falta de APs novos.

Aquisição de Equipamentos de TI contempla a renovação de parques de máquinas obsoletos através de SRP.

Eixo 2: Modernização de Sistemas Legados

Modernização ou aquisição de sistema acadêmico/administrativo por sistema mais moderno é prioritária. O SIE é um sistema legado com limitações operacionais significativas, em especial na utilização pelas Pró-Reitorias, falta de sistema web adequado e responsivo, falta de integração com sistemas do governo federal, entre outros. As soluções propostas envolvem a aquisição e a migração para um novo sistema como o SUAP (Sistema Unificado da Administração Pública) ou o SIGA, que oferecem plataforma moderna, arquitetura escalável e alinhamento ao PDI 2026-2030. Os principais desafios incluem custo de aquisição (caso do SIGA, principalmente), customizações necessárias, migração de dados históricos e treinamento extensivo dos usuários.

Implementação de Sistemas Integrados de Gestão, utilizando-se de sistemas administrativos integrados como o SUAP ou SIGA. Os componentes incluem sistemas de gestão de custos, SIADS, recursos humanos, orçamento e planejamento institucional.

Expansão da Inteligência Artificial no SAUIM e demais sistemas institucionais, que

prevê novas modalidades de análise acadêmica, enfrentando desafios relacionados à qualidade de dados e necessidade de refinamento contínuo dos modelos preditivos, e até uso de LLMs em sistemas como SAUIM ou ECampus

Ampliação da Modernização de Processos da Pós-Graduação usando o sistema ECampus para o auxílio e expansão das ações da Pós-Graduação como oferta, solicitação de matrícula, integração com o sucupira (GoPG), entre outros.

Expansão das atividades da Extensão no ECampus através da implementação dos formulários de submissões de projetos relacionados à extensão no ecampus.

Aprimoramento da Assistência Estudantil no ECampus através da implementação adequada e atualizada do sistema CadUFAM e da assistência estudantil conforme as novas regras a serem estabelecidas para assistência estudantil na UFAM.

Eixo 3: Segurança da Informação

A segurança da informação representa desafio contínuo e estratégico, especialmente considerando que em 2025 foi estabelecido efetivamente a Equipe de Tratamento de Incidentes de Rede (ETIR) e a Política de Acesso a Recursos de TIC, entre outras instruções do PPSI, no 5o ciclo. Os principais desafios para 2026 incluem:

Avanço no Programa Permanente de Segurança da Informação (PPSI) além do Ciclo 5 alcançado em 2025, o PPSI está sendo atualizado para o chamado PPSI 2.0 em 2026, assim, é necessário aprofundar a implementação de controles de segurança, expandir as auditorias de conformidade à LGPD e fortalecer continuamente as políticas de classificação e proteção de dados institucionais, conforme estabelecido nas boas práticas e normas do PPSI.

Fortalecimento e Ampliação da ETIR para atender ao crescente volume e complexidade de incidentes de segurança. Considerando os 59 incidentes tratados em 2025, projeta-se aumento significativo com a expansão dos serviços digitais. Além disso, é necessário capacitação contínua da equipe, aquisição de ferramentas avançadas de detecção e resposta, e estabelecimento de protocolos ágeis (e publicização) de tratamento de incidentes críticos.

Expansão das Campanhas de Conscientização em segurança da informação para atingir efetivamente toda a comunidade universitária. Embora campanhas sobre phishing, engenharia social e proteção de dados já tenham sido realizadas, o desafio é criar programas permanentes e mensuráveis, com treinamentos obrigatórios periódicos e avaliações de efetividade, reduzindo o fator humano como vetor de vulnerabilidade.

Aprimoramento de Controles de Acesso e Autenticação através da expansão da autenticação multifator (MFA) para todos os sistemas institucionais, não apenas os críticos. Implementar gestão de identidade mais robusta (IAM - Identity and Access Management), incluindo revisão automatizada de permissões, segregação de funções mais rigorosa e auditoria contínua de acessos privilegiados.

Modernização da Infraestrutura de Backup expandindo a solução Veeam de backup, além da realização de testes periódicos de restauração completa de ambientes críticos.

Conformidade Regulatória e Governança visando atender às crescentes exigências de órgãos de controle (CGU, TCU) quanto à segurança de dados governamentais e transparência nos processos de proteção de informações sensíveis.

Eixo 4: Conformidade com o PDI 2026-2030

O eixo de segurança da informação apresenta novas metas alinhadas ao PDI 2026-2030 (OE 11), com desafios específicos em cada frente:

Meta M1 - Atender 100% das 10 soluções críticas de segurança: partindo de 0% em 2025, a meta é atingir 100% em 2026. O principal desafio é a identificação precisa dessas soluções críticas e priorização dos investimentos necessários.

Meta M2 - Monitorar 100% dos SLAs (Service Level Agreements): com 60% de cobertura em 2025, busca-se atingir 100% em 2026. O desafio principal é a instrumentação de todos os serviços com ferramentas adequadas de monitoramento.

Meta M3 - Avaliar 100% dos serviços de TI: partindo de 75% em 2025, a meta é totalizar 100% em 2026 através de coleta contínua de feedback dos usuários e análise sistemática de qualidade.

Meta M4 - Manter 99% de disponibilidade dos serviços críticos: atualmente não quantificado, e que representa o desafio de implementar infraestrutura redundante e protocolo robusto de resposta a incidentes.

Meta M5 - Infraestrutura em 100% das unidades: expansão essa necessária e demandada, mas que exigem em parte a aquisição de equipamentos como Switch Core, Switches para unidades e APs para expansão WiFi.

Meta M6 - Adequação ao Instrumento de Desenvolvimento de Gestão (IDG-2019): partindo de 0% de adequação em sites institucionais, a meta é atingir 20% em 2026, o que demandará redesign de portais para conformidade com padrões de acessibilidade e usabilidade.

3. Quais as leis, resoluções, decisões normativas e atos normativos que regem a gestão da tecnologia da informação na UFAM?

A gestão da tecnologia da informação na UFAM está subordinada a um arcabouço normativo que integra legislação federal, decretos presidenciais, instruções normativas do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), normas de segurança da informação do Gabinete de Segurança Institucional (GSIPR) e atos normativos internos institucionais.

No âmbito dos normativos internos, destacam-se as Políticas como a PoSIC, de Controle de Acesso a Recursos de TIC, a Resolução que rege o CGD, entre outras, destacadas a seguir.

A Política de Segurança da Informação e Comunicações (PoSIC) da UFAM constitui a declaração formal do comprometimento da instituição com a proteção de informações. Esta política é vinculante para todos os servidores técnico-administrativos e docentes, colaboradores, consultores externos, prestadores de serviços, estagiários e discentes que exerçam atividades no âmbito da UFAM ou quem quer que tenha acesso a dados ou informações no ambiente institucional. Seu propósito é estabelecer diretrizes, normas e procedimentos, atribuindo responsabilidades e competências adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes à UFAM.

A Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação e Comunicação foi aprovada e implementada em 2025 com a finalidade de regulamentar o uso e o acesso aos recursos de TIC mantidos pela UFAM. Esta instrução normativa integra e operacionaliza a PoSIC, cumprindo requisitos federais de LGPD e segurança, disciplinando especificamente o acesso à rede de dados institucional e o acesso a sistemas institucionais. A política estabelece que os recursos devem ser utilizados exclusivamente para fins de ensino, pesquisa, extensão e administração, conforme missão e princípios da UFAM.

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação da UFAM tem como objetivo estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar os servidores e sensibilizar a comunidade acadêmica que em algum momento têm acesso ou realizam operações de tratamento de dados pessoais. Esta política visa manter um programa de conscientização contínua com ênfase em privacidade e segurança da informação, educando os usuários da instituição sobre como interagir com ativos e dados corporativos e pessoais de maneira segura, garantindo o entendimento, conhecimentos e comportamentos necessários para ajudar a manter a segurança pessoal e da instituição.

A Portaria de Uso do Google Workspace institui as normas operacionais para que o uso do serviço de armazenamento de dados em nuvem dos serviços Google da UFAM esteja alinhada à Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação da UFAM. Esta portaria define as responsabilidades dos usuários, estabelece limites de uso, orienta sobre boas práticas de segurança, proteção de dados e conduta ética, além de promover a padronização de procedimentos.

A Resolução nº 014, de 11 de março de 2025, aprova o Regimento Interno do Comitê de Governança Digital (CGD/UFAM) pelo Conselho de Administração (CONSAD), estabelecendo a estrutura de governança de TI da universidade. O CGD constitui o máximo órgão de deliberação sobre políticas e estratégias de TI da UFAM, sendo composto por pró-reitores, diretores de unidades acadêmicas e administrativas, diretor do CTIC e representantes de discentes e servidores. As funções principais do CGD incluem aprovar a implementação de novos sistemas e soluções de TI, definir prioridades de investimento anual em TI, validar e aprovar o PDTI (Plano Diretor de TI) e PTD (Plano de Transformação Digital), e deliberar sobre políticas institucionais de TI.

A Portaria nº 2, de 3 de janeiro de 2025, estabelece os procedimentos internos de contratação vigentes desde janeiro de 2025, sob autoridade da Pró-Reitora de Administração e Finanças, com ênfase no seguinte termo: que para aquisição de bens e contratação de serviços de TIC, a equipe de planejamento deve conter um técnico disponibilizado pelo Centro de Tecnologia de Informação e Comunicação - CTIC - UFAM, e que a futura aquisição/contratação deva estar contemplada no PDTIC e Plano de Contratações Anual - PCA. Este requisito garante que todas as contratações de TI passem por análise técnica especializada do CTIC, estejam alinhadas ao planejamento estratégico de tecnologia da instituição e sejam devidamente priorizadas e orçadas no planejamento anual, evitando contratações desalinhadas, redundantes ou tecnicamente inadequadas.

O Ofício Circular nº 01/2023/CTIC/UFAM, emitido em 27 de junho de 2023, divulga o Catálogo de Serviços de TIC com objetivo de divulgar os serviços ativos disponíveis e os procedimentos padronizados para solicitação através da Central de Serviços (suportectic.ufam.edu.br) como canal de atendimento único para atendimento ao usuário. Os procedimentos de solicitação estabelecem que serviços normais devem ser solicitados via Central de Serviços, enquanto que serviços envolvendo desenvolvimento ou alteração de sistemas devem ser solicitados via SEI/UFAM. Para solicitações de desenvolvimento ou alteração de sistemas, o processo envolve preenchimento de Documento Oficial de Demanda de Soluções de TIC, envio para a Coordenação de Projetos e Processos (CPROJPROC) do CTIC, análise de viabilidade técnica, alinhamento ao PDTIC e priorização pelo Comitê de Governança Digital.

4. Qual o montante de recursos aplicados em tecnologia da informação na UFAM?

Os recursos aplicados em TICs na UFAM, geridos pelo CTIC, são detalhados nos itens 5 e 6 deste relatório. Assim, a tabela a seguir apresenta o montante de recursos aplicados em naturezas de despesa relacionadas a TICs, mas não geridos/mantidos pelo CTIC e/ou oriundo de ações de outras unidades da UFAM.

Unidade	Bem de TI adquirido	Valor R\$ (Despesa Empenhada)
PROADM	M0006Q0100N-CTT - SOFTWARE SERVICOS FISCAIS	23.400,00
PROADM	M0027Q0100N-CTT - SERVICO DE CERTIFICADOS DIGITAIS	8.332,23
ISB	M20RKG7233N-IFES SEM HU (Minha biblioteca de ISB)	57.410,00
Biblioteca Central	M0041Q0100N-CTT - SISTEMA DE BIBLIOTECA (Pergamum)	31.217,33
Biblioteca Central	M0041Q0101N-CTT - SISTEMA DE BIBLIOTECA - NORMA TECNICA (Base de dados Target)	20.000,00
Biblioteca Central	M0041Q0102N-CTT - SISTEMA DE BIBLIOTECA - MANUTENCAO	2.450,50
PROPLAN	M0099Q0100N-DESPESAS EVENTUAIS	17.280,00
PCU	M0019Q0100N-CTT - SISTEMA ORCAFACIL	12.389,00
PROAE	M4002G2396N-PROAE - DESPESAS DIVERSAS (Serviço de infraestrutura de rede)	16.685,00

	TOTAL	189.164,06
--	--------------	------------

5. Quantas e quais são as contratações (serviços e equipamentos) mais relevantes de tecnologia da informação na UFAM? (total)

Os contratos mantidos e geridos pelo CTIC (11 contratos) são apresentados na tabela a seguir, seguindo a dotação orçamentária atualizada do final do ano-base de 2025, não considerando-se, para fins deste relatório, a dotação planejada, conforme dados extraídos dos painéis orçamentários disponíveis no site da PROPLAN/UFAM.

Bem de TI / Serviço	Dotação Atualizada (R\$)	Valor Empenhado (R\$)	% Empenhado
Sistema SIE	696.394,94	696.394,94	100%
Serviços de Computação em Nuvem (Serpro)	421.062,48	421.062,48	100%
Manutenção de Redes Ópticas	225.076,03	225.076,03	100%
Serviços de Internet e Telefonia (100N)	212.357,28	212.357,28	100%
Suporte de Hard. e Soft. Datacenter (HPE)	205.825,64	205.825,64	100%
Serviços de Garantia de Equip. DE TIC (HPE)	110.257,41	110.257,41	100%
Serv. e Manutenção de Backup de Dados (Veeam)	62.725,44	62.725,44	100%
Plataforma Digital de Aperfeiçoamento TIC	36.526,66	36.526,66	100%
Software de Licença VPN	32.195,58	32.195,58	100%

Serviços de Internet e Telefonia (101N)	128,98	28,98	22,47%
Google Workspace - REDE NACIONAL DE ENSINO E PESQUISA - RNP (apenas gestão contratual do CTIC)	375.400	375.400	100%

6. Quantas e quais são as contratações (serviços e equipamentos) mais relevantes de tecnologia da informação na UFAM? (realizada no ano base)

Conforme apresentado no item 5 do presente relatório, 11 contratos foram mantidos pelo CTIC em 2025, e nenhum equipamento de TI foi adquirido pelo CTIC no ano de 2025. Além disso, ressalta-se que dos 11 contratos, 2 são novos contratos: Serv. e Manutenção de Backup de Dados (Veeam) no valor de R\$ 62.725,44 e Google Workspace - REDE NACIONAL DE ENSINO E PESQUISA - RNP (apenas gestão contratual do CTIC), no valor de R\$ 375.400,00.

7. Quantos foram os serviços executados (de suporte ao usuário, de rede, de manutenção em sistema, de gestão de segurança da informação) e projetos em matéria de tecnologia da informação na UFAM?

Serviços de Rede

Durante o ano de 2025, foram executados serviços abrangentes de infraestrutura de rede no âmbito do Contrato 07/2022 (Termo Aditivo 03/2025), contemplando instalação de pontos de rede, patch panels, racks e cabeamento estruturado em fibra óptica.

Resumo quantitativo:

- **Total de pontos de rede instalados:** Mais de 500 pontos
- **Patch panels instalados:** 15 unidades
- **Racks instalados:** 3 unidades
- **Cabeamento óptico instalado:** 684 metros (12 fibras)
- **Fusões e conectorizações:** 6 procedimentos

Distribuição completa dos serviços executados:

LOCAL DA EXECUÇÃO DO SERVIÇO	DESCRIÇÃO DO SERVIÇO	PERÍODO
FACULDADE DE TECNOLOGIA - FT Bloco Administrativo 2º andar - Centro Acadêmico de Engenharia de Produção Bloco Pós-Graduação Térreo - PPG Engenharia Mecânica Bloco Prof. Vilar Câmara Sala do PPG Design Auditórios da FT Auditório Rio Javari Auditório Rio Jutai Bloco Laboratório de Saneamento Sala das Técnicas	Reinstalação de 1 ponto de rede Instalação de 27 pontos de rede novos Instalação de 2 patch panels Instalação de 6 pontos de rede novos Instalação de 2 pontos de rede novos Instalação de 2 pontos de rede novos Instalação de 3 pontos de rede novos	Fevereiro/2025
INSTITUTO DE CIÊNCIAS EXATAS Bloco Departamento Geociências Térreo - Laboratório de Geofísica 1º andar - Laboratório de Microscopia Bloco Departamento de Estatística	Instalação de 10 pontos de rede novos Instalação de 1 patch panel	Fevereiro/2025

Térreo - Sala de Reuniões Bloco Departamento Química 2º andar - Secretaria do PPPGQ	Instalação de 2 pontos de rede novos Instalação de 2 pontos de rede novos Instalação de 2 pontos de rede novos	
FACULDADE DE ESTUDOS SOCIAIS Bloco de salas de aula 2 Sala 61	Instalação de 2 pontos de rede novos Instalação de 1 patch panel	Fevereiro/2025
FACULDADE DE ARTES 1º andar - sala 67	Instalação de 2 pontos de rede novos	Fevereiro/2025
FACULDADE DE DIREITO Bloco Administrativo Biblioteca Térreo - corredor Bloco do Centro Acadêmico Térreo - corredor	Instalação de 1 ponto de rede novo Instalação de 3 pontos de rede novos para wifi Instalação de 2 pontos de rede novos para wifi	Fevereiro/2025
INSTITUTO DE CIÊNCIAS BIOLÓGICAS Bloco 1 Térreo - Sala de cultura de tecidos 2º andar- Laboratório de Morfologia Quantitativa Bloco 2 3º andar - Laboratório de Fisiologia Humana	Instalação de 2 pontos de rede novos Instalação de 2 pontos de rede novos Instalação de 1 ponto de rede novo	Fevereiro/2025
INSTITUTO DE EDUCAÇÃO, AGRICULTURA E AMBIENTE - IEAA BLOCO 3 Pavimento 1 ----- Pavimento 2 ----- Pavimento 3 -----	Instalação de 49 pontos de rede novos Instalação de 2 Patch Panels Instalação de 7 pontos de rede novos Instalação de 2 Racks de Parede 19" 12U Instalação de 1 Patch Panel Instalação de 15 pontos de rede novos Instalação de 1 patch panel Instalação de 19 pontos de rede novos Instalação de 1 patch panel Instalação de 8 pontos de rede novos	Fevereiro/2025

Pavimento ----- ----- RESTAURANTE UNIVERSITÁRIO ----- GALPÃO GARAGEM ----- -----	4	Instalação de 1 rack parede 19" 12U Instalação de 1 patch panel Instalação de 184m de cabo óptico Instalação de 2 conectorizações de cabo óptico Instalação de 10 pontos de rede novos Instalação de 1 rack parede 19" 12U	
FACULDADE DE TECNOLOGIA - FT Bloco Rio Canumã Coordenação dos Laboratórios de Informática - LIFTs		Instalação de 4 pontos de rede novos Instalação de 1 patch panel	Março/2025
FACULDADE DE EDUCAÇÃO - FAGED Bloco Faced1 1º andar - Sala de Licenciatura Indígena		Reinstalação de 3 pontos de rede	Março/2025
CENTRO DE CONVIVÊNCIA Térreo - sala 02 Térreo - sala 03 Sala da PROAE		Instalação de 3 pontos de rede novos Instalação de 5 pontos de rede novos Instalação de 4 pontos de rede novos	Março/2025
FACULDADE DE EDUCAÇÃO FÍSICA E FISIOTERAPIA - FEFF Bloco C 1º andar - PRODAGIN		Instalação de 5 pontos de rede novos	Março/2025
FACULDADE DE CIÊNCIAS AGRÁRIAS - FCA Bloco V Laboratório ÁRVORE-LAB Laboratório de Tecnologia da Madeira		Instalação de 7 pontos de rede novos Instalação de 1 patch panel Instalação de RACK de telecomunicações	Março/2025
BLOCO CAIS Sala do Serviço Social Antiga sala de reuniões		Instalação de 2 pontos de rede novos Reinstalação de 1 ponto de rede	Março/2025
BLOCO COMPEC Salão de entrada		Instalação de 6 pontos de rede novos	Março/2025
FACULDADE DE ODONTOLOGIA Corredores do 1º, 2º, 3º e 4º andares 2º andar - Laboratório de Pesquisa		Instalação de 4 pontos de rede novos para câmeras Instalação de 1 ponto de rede novo	Março/2025

	Reinstalação de 1 ponto de rede	
FACULDADE DE EDUCAÇÃO - FAGED Bloco FAGED3 térreo - Sala da Coordenação de manutenção predial	Instalação de 2 pontos de rede novos	Junho/2025
CENTRO DE CONVIVÊNCIA PROAE - salas 8 e 9	Instalação de 4 pontos de rede novos	Junho/2025
INSTITUTO DE CIÊNCIAS EXATAS Bloco da Física - sala da chefia Bloco da Estatística - térreo - laboratório de Estatística	Instalação de 2 pontos de rede novos Instalação de 1 ponto de rede novo	Junho/2025
BLOCO IFCHS1 Térreo e 1º andar	Reinstalação de 1 ponto de rede	Junho/2025
REITORIA 1º andar - sala da Diretoria Executiva	Instalação de 1 ponto de rede novo	Junho/2025
FACULDADE DE EDUCAÇÃO FÍSICA E FISIOTERAPIA - FEFF Bloco C - térreo - LABTAM	Instalação de 1 ponto de rede novo	Junho/2025
FACULDADE DE CIÊNCIAS AGRÁRIAS - FCA - Bloco U Centro Acadêmico de Agronomia Sala dos TAES	Instalação de 2 pontos de rede novos Instalação de 2 pontos de rede novos	Junho/2025
BLOCO CAIS Sala da secretaria	Instalação de 1 ponto de rede novo	Junho/2025
BLOCO PÓS-BIOAGRO 3º andar - Laboratório de Genômica	Instalação de 6 pontos de rede novos	Junho/2025
BLOCO C - SETOR SUL Grupo de Estudo e Pesquisa - GETRA	Instalação de 1 ponto de rede novo	Junho/2025
BLOCO DA PREFEITURA DO CAMPUS Coordenação de Projetos e Fiscalização de Obras e gabinete do prefeito	Instalação de 8 pontos de rede novos Reinstalação de 1 ponto de rede	Junho/2025
BLOCOS LAPEC-COMPEC Trecho entre os dois blocos	Instalação de 200 metros de cabo óptico aéreo	Junho/2025
FCA - AVIÁRIO	Confecção de 2 fusões em fibra óptica	Junho/2025
FACULDADE DE ODONTOLOGIA 2º andar - Laboratório de Pesquisa	Instalação de 1 ponto de rede novo	Junho/2025
FACULDADE DE MEDICINA		

Térreo - DPML	Instalação de 5 pontos de rede novos	Junho/2025
ESCOLA DE ENFERMAGEM Sala 3 Sala 25 Sala 29 Sala 39 Sala 47 Miniauditório	Instalação de 2 pontos de rede novos Instalação de 1 ponto de rede novo Instalação de 1 ponto de rede novo Reinstalação de 1 ponto de rede Instalação de 1 ponto de rede novo Instalação de 1 ponto de rede novo Instalação de 1 ponto de rede novo	Junho/2025
FAZENDA EXPERIMENTAL Laboratório de Energia Solar - CDEAM Laboratório de Produção de Etanol - CDEAM	Instalação de 3 pontos de rede novos Instalação de 3 pontos de rede novos	Agosto/2025
BLOCO FARMÁCIA VIVA - FCF	Instalação de cabo óptico aéreo, 12 fibras, e respectivos acessórios, no trecho entre os prédios do Projeto Farmácia Viva e o LAPEC. Fusões ópticas na fibra, sendo 2 em cada extremidade, total de 4.	Setembro/2025
INSTITUTO DE EDUCAÇÃO, AGRICULTURA E AMBIENTE - IEAA	Instalação de 100 metros de cabo óptico aéreo, 12 fibras, e conectorização no DIO, no trecho entre o Restaurante Universitário e o Galpão-garagem	Novembro/2025

Esses serviços atenderam demandas de expansão de laboratórios de pesquisa, salas de aula, setores administrativos, sistemas de segurança (câmeras) e cobertura WiFi, garantindo conectividade adequada para as atividades acadêmicas e administrativas da universidade.

Serviços de atendimento ao usuário

O serviço de suporte técnico do CTIC atendeu **1.849 chamados** em 2025 através do sistema GLPI (Portal de Serviços de TIC do CTIC/UFAM), com os dados consolidados abaixo.

Indicadores de Desempenho GLPI:

- **Total de chamados:** 1.849
- **Taxa de resolução:** 99,5% (1.839 chamados fechados)
- **Tempo médio de resolução:** 3,1 dias (73,3 horas)

- **Tempo mediano de resolução:** 1 dia (24 horas)
- **Chamados em atendimento:** 5 (0,3%)
- **Chamados pendentes:** 4 (0,2%)

Distribuição por Tipo de Chamado:

- **Requisições:** 1.619 chamados (87,6%)
- **Incidentes:** 230 chamados (12,4%)

Principais Categorias de Atendimento do GLPI:

- **Equipamentos de TIC:** 466 (25,2%) - Manutenção, instalação e configuração de hardware
- **Sistemas Institucionais:** 436 (23,6%) - Atribuição de perfis, novos usuários, relatórios
- **Recursos de TIC:** 155 (8,4%) - Instalação de software, problemas técnicos
- **Gestão de E-mail:** ~280 (15%) - Criação, migração, desbloqueio, recuperação de senha
- **Rede e Conectividade:** 29 (1,6%) - Falhas de rede, manutenção de pontos
- **Portais Institucionais:** 29 (1,6%) - Problemas de acesso e configuração
- **Compartilhamento de Arquivos:** 22 (1,2%) - Permissões e acessos a repositórios
- **Outros:** 185 (10,0%) - Demandas diversas

Distribuição Mensal de Chamados:

- Janeiro: 159 chamados
- Fevereiro: 214 chamados
- Março: 169 chamados
- Abril: 156 chamados
- Maio: 134 chamados
- Junho: 160 chamados
- Julho: 225 chamados
- Agosto: 179 chamados
- Setembro: 131 chamados
- Outubro: 139 chamados
- Novembro: 119 chamados
- Dezembro: 64 chamados

Gestão de Projetos de TIC

O CTIC gerenciou em 2025 um conjunto de **11 contratos estratégicos** de TIC, garantindo a continuidade operacional dos serviços de TIC da instituição com as dotações planejadas (não atualizadas conforme os itens 5 e 6 deste relatório) são apresentados em detalhes:

Novas Contratações (2025):

- **Licença Veeam Backup & Replication** - Lanlink Informática: R\$ 62.725,44
Solução de backup e recuperação de desastres
- **Google Workspace Education Plus** - RNP: R\$ 375.400,00
Plataforma de produtividade e colaboração (gestão contratual em conjunto com a PROEG/UFAM)

Renovações de Contratos:

- **Redes Ópticas** - ERA Engenharia: R\$ 885.719,94
Manutenção e gerenciamento da infraestrutura de fibra óptica
- **VPN NGFW** - Teltec Solutions: R\$ 32.195,58
Firewall de nova geração e VPN corporativa
- **Sistema Integrado de Ensino (SIE)** - AVMB Tecnologia: R\$ 733.780,56
Sistema acadêmico institucional
- **Suporte Técnico Datacenter HPE** - HPE: R\$ 158.090,04
Suporte técnico especializado para servidores e storage
- **Garantia Estendida HPE** - HPE: R\$ 170.369,64
Garantia de hardware para equipamentos críticos
- **Cloud Computing Serpro** - Serpro: R\$ 1.642.805,88
Infraestrutura em nuvem para sistemas institucionais
- **Plataforma Alura Educação** - AOVS Sistemas: R\$ 27.400,00
20 licenças para capacitação em tecnologia para os servidores do CTIC
- **Telefonia Móvel TIM** - TIM: R\$ 539.125,71
Serviços de telefonia móvel corporativa
- **Telefonia Móvel Claro** - Claro: R\$ 78.151,50
Serviços de telefonia móvel corporativa

Valor Total Gerenciado: R\$ 4.330.364,29

Serviços de Manutenção de Sistemas

Quanto a serviços de manutenção de sistemas, registrados no GLPI, em 2025 foram **1514 (dos quais 1426, 94%, foram fechados/solucionados) chamados** relacionados à manutenção de sistemas, relatórios de sistemas ou mudanças de funcionalidades nos sistemas.

Serviços de Gestão de Segurança da Informação

Por fim, na relação de ações de segurança da informação, foram realizadas 6 categorias principais de ações de segurança da informação em 2025: PPSI Ciclo 5, estabelecimento da ETIR - Equipe de Tratamento de Incidentes de Rede (com tratamento de 59 incidentes de segurança da informação), Campanhas de Conscientização com 6 temas abordados (phishing, engenharia social, senhas, LGPD, e-mail corporativo, home office), Auditorias e conformidades como adequações à LGPD, Controles de Acesso com 5 melhorias

implementadas (MFA, revisão de perfis, política de senhas, desativação automática, segregação de funções) e Backup/Recuperação.

Os detalhes das ações de segurança da informação são detalhados no item 8 do presente relatório.

8. Quais as ações executadas sobre segurança da informação na UFAM.

1. DESENVOLVIMENTO DO INDICADOR DE SEGURANÇA DA INFORMAÇÃO (ISEG) DO PPSI NA UNIVERSIDADE

Descrição:

- A Secretaria de Governo Digital do Ministério de Inovação em Serviços Públicos solicita às instituições pertencentes ao SISP que implementem **controles e medidas** do **Programa de Privacidade e Segurança da Informação (PPSI)** e realizem estudo de autodiagnóstico semestralmente em ciclos.

1.1. Consolidação do Ciclo 5 do autodiagnóstico do PPSI

Ações:

- **Consolidação das respostas das 310 medidas de Segurança da Informação que compõem o iSeg**, de acompanhamento na universidade pela CSEGINFO.
- Acompanhamento junto ao **Escritório de Proteção de Dados Digitais**, com a sra. Encarregada de Dados Nycolle e suplente Rafael, sobre alinhamento de **envio a SGD/MCI do Ciclo 5 do autodiagnóstico do PPSI** com as **medidas iSEG e iPRIV consolidadas**.
- Encaminhamentos registrados no processos SEI n. 23105.031436/2025-34

1.2. Garantia de adequado planejamento dos controles iSEG no PDI da UFAM

Ações:

- Encaminhamentos junto à nova diretoria do CTIC para proposição de melhorias no planejamento da Segurança da Informação na instituição, incluindo a **transferência do indicador de Segurança da Informação (iSEG) do eixo de Tecnologia da Informação para o eixo de Governança no Plano de Desenvolvimento Institucional (PDI) 2026-2030 da universidade**.
- Alinhamento com **Departamento de Planejamento Estratégico da PROPLAN** a acerca do desenvolvimento do **planejamento do iSEG** no âmbito do **Comitê de Governança Digital** da instituição.
- Registro da efetividade da ação através da publicação do **PDI 2026-2030** no site da **PROPLAN**:

<https://drive.google.com/file/d/1IerHngUSI-j99JfIgeYPBaQuzeg4p1WN/view>

6. GOVERNANÇA		UNIVERSIDADE FEDERAL DO AMAZONAS	
OBJETIVO ESTRATÉGICO		6.6 Objetivos, Metas e Indicadores	
6.6		6.6.6 Governança	
<p>Promover a cultura de proteção de dados e segurança da informação, orientando e fiscalizando o cumprimento da Lei Geral de Proteção de Dados (LGPD) e do Programa de Privacidade de Segurança da Informação (PPSI), a fim de assegurar a privacidade dos titulares de dados pessoais e a disponibilidade, integridade, confidencialidade e autenticidade das informações institucionais.</p> <p>ODS 16 - Paz, Justiça e Instituições</p>		META	INDICADOR
		Nome do Indicador	Fórmula do Cálculo *NA = não se aplica
		M1 - OE 6.6 - Promover duas capacitações por ano acerca da Lei nº 13.709/2018 (LGPD), buscando a conscientização sobre o tema, em 100% das unidades e órgãos, até 2030.	I1 - M1 - OE 6.6 - Capacitações realizadas NA*
		M2 - OE 6.6 - Avaliar anualmente, 100% das unidades e órgãos de acordo com o "Ranking de capacitação em LGPD", até 2030.	I2 - M2 - OE 6.6 - Avaliação realizada NA*
		M3 - OE 6.6 - Realizar um levantamento anual das ferramentas de inteligência artificial (IA) que podem ser úteis para otimizar processos administrativos e acadêmicos na Universidade, incluindo ferramentas para tradução e adaptação das normativas da Universidade para pessoas com deficiência, até 2030.	I3 - M3 - OE 6.6 - Levantamento realizado NA*
		M4 - OE 6.6 - Elaborar e aprovar bianualmente o Plano Diretor de Tecnologia da Informação (PDTI), até 2030.	I4 - M4 - OE 6.6 - PDTI elaborado NA*
		M5 - OE6.6 - Elevar em 50% o índice de gestão da segurança da informação (iSeg), de acordo com os parâmetros do PPSI, até 2030.	I5 - M5 - OE6.6 - Índice iSeg FC1 - I5 - M5 - OE6.6 - Considerar fórmula de alcance do índice
		M6 - OE6.6 - Elevar em 50% o índice de privacidade (iPriv), de acordo com os parâmetros do PPSI, até 2030.	I6 - M6 - OE6.6 - Índice iPriv FC2 - I6 - M6 - OE6.6 - Considerar fórmula de alcance do índice

1.3. Ações da Segurança da Informação voltadas à conformidade com o PPSI

Ações:

- Produção e atualização de **normativos institucionais**, com a elaboração de minutas a serem submetidas à apreciação, a saber: Minuta Política de Gestão de Registros de Logs, Minuta Política de Utilização de Softwares e Minuta da Política de Backup e Restauração de Dados Digitais.
- Encaminhamento à direção do CTIC de **manifestações de caráter técnico e consultivo**, referentes ao atendimento dos Controles 1, 2 e 10 do PPSI. As manifestações tiveram por objetivo fornecer subsídios técnicos quanto à **conformidade e aos riscos envolvidos**, bem como fundamentar o processo decisório e as aprovações pertinentes pela **alta gestão**, apoiando a direção do CTIC no planejamento e no direcionamento das providências junto às **áreas operacionais de TI** responsáveis pela gestão dos ativos relacionados. **Parecer técnico de conformidade** encaminhado nos processos SEI n. 23105.042786/2025-26 (Controles 1 e 2) e 23105.041051/2025-85 (Controle 10).

2. DESENVOLVIMENTO DO PROCESSO DE TRATAMENTO E RESPOSTA A INCIDENTES

2.1. Aprovação do Plano de Tratamento e Resposta a Incidentes da Universidade Federal do Amazonas



Ações:

- Elaboração e encaminhamentos para aprovação do **Plano de Gestão de Incidentes de Segurança da Informação** da Universidade Federal do Amazonas junto ao **Comitê de Governança Digital**.
- Registros no site da UFAM de 12 de Maio de 2025. Link: <https://ufam.edu.br/noticias-destaque/6660-em-reuniao-comite-de-governanca-digital-aprova-plano-de-gestao-de-incidentes-da-ufam.html>

2.2. Estabelecimento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da Universidade Federal do Amazonas

Ações:

- Encaminhamentos para o **estabelecimento da ETIR na universidade** através da indicação dos membros junto a Reitoria, culminando na publicação da Portaria GR/UFAM nº 2799, de 04 de dezembro de 2025.
- Encaminhamentos registrados no Processo SEI n. 23105.018410/2025-09 e 23105.033322/2025-29.



Ministério da Educação
Universidade Federal do Amazonas
Gabinete da Reitora

Boletim de Serviço Eletrônico em 10/12/2025

PORTARIA Nº 2799, DE 04 DE DEZEMBRO DE 2025

A REITORA DA UNIVERSIDADE FEDERAL DO AMAZONAS, usando das atribuições estatutárias, conferidas por Decreto de 1º de julho de 2025, publicado no Diário Oficial da União de 02 de julho de 2025, e

CONSIDERANDO a competência estabelecida no Inciso XVI do Artigo 19 do Estatuto da Universidade Federal do Amazonas;

CONSIDERANDO a Instrução Normativa GSI/PR Nº 1/2020, 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 e criação de Equipes de Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Administração Pública Federal;

CONSIDERANDO a Resolução CGD nº 01/2025, de 18 de junho de 2025, que instituiu o Plano de Gestão de Incidentes de Segurança da Informação da Universidade Federal do Amazonas (UFAM);

CONSIDERANDO a instrução dos autos do Processo SEI nº 23105.018410/2025-09,

R E S O L V E:

Art. 1º. DESIGNAR os servidores abaixo para integrar a Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR da Universidade Federal do Amazonas:

I. COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO – CSEGINFO:

Agente Responsável pela ETIR:

Analista de Tecnologia da Informação LENDEL DOS SANTOS MONTEIRO – CTIC
Matrícula SIAPE nº 3396521

Agente Responsável pela ETIR Adjunto:

Analista de Tecnologia da Informação JORGE CARLOS MAGNO SILVA DE LIMA – CTIC
Matrícula SIAPE nº 2380702

1º TITULAR:

Analista de Tecnologia da Informação JORGE CARLOS MAGNO SILVA DE LIMA – CTIC
Matrícula SIAPE nº 2380702

TITULAR ADJUNTO:

Técnico(a) de Laboratório Informática GILBERTO AIRES LIBANIA – CTIC
Matrícula SIAPE nº 1752725

2.3. Fortalecimento das ações da ETIR

Ações:

- Atuação direta no apoio às ações do ETIR, com **desenvolvimento e aprimoramento de procedimentos internos de Segurança da Informação**, visando padronizar o tratamento e a resposta a incidentes no âmbito da instituição.
- Acompanhamento, análise e tratamento das ocorrências de incidentes de Segurança da Informação reportadas pelos grupos de resposta a incidentes **CTIR.gov**, **Centro Integrado de Segurança Cibernética (CISC)** e **CAIS-RNP**.
- Monitoramento contínuo das ocorrências, incluindo registro, mitigação dos riscos identificados e acompanhamento das ações corretivas adotadas pelas áreas envolvidas.
- Encaminhamento, pelo time da CSEGINFO, de **59 ocorrências de incidentes de Segurança da Informação** ao longo do ano de 2025. Indicadores registrados no sistema GLPI.



3. DESENVOLVIMENTO DO PROCESSO DE CONTROLE DE ACESSO

3.1. Aprovação da Política de Controle de Acesso à Informação e aos Recursos de TIC

Ações:

- Acompanhamento junto ao conselho superior da universidade e providências de correções finais para a publicação.
- Encaminhamentos registrados no Processo SEI n. 23105.038246/2023-86.

BRASIL Simplifique! Comunica BR Participe Acesso à Informação Legislação Canais

UFAM UNIVERSIDADE FEDERAL DO AMAZONAS

Assessoria de Comunicação Carta de Serviços ao Usuário Fale Conosco Webmail

PÁGINA INICIAL > NOTÍCIAS > UFAM APROVA POLÍTICA DE CONTROLE DE ACESSO À INFORMAÇÃO E AOS RECURSOS DE TIC E INICIA OBRIGATORIEDADE DE AUTENTICAÇÃO EM DOIS FATORES

Ufam aprova Política de Controle de Acesso à Informação e aos Recursos de TIC e inicia obrigatoriedade de autenticação em dois fatores

Acesso: 512

A Universidade Federal do Amazonas (Ufam), dia 13 de novembro, aprovou a [Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação e Comunicação](#), elaborada pela Coordenação de Segurança da Informação do Centro de Tecnologia da Informação e Comunicação (CTIC). A medida, aprovada pela Resolução nº 014/2025, do Conselho Universitário, é um importante passo na garantia da Segurança de Informação para toda comunidade acadêmica e representa um avanço importante na modernização da governança digital da Ufam.

A nova política estabelece diretrizes para proteger contas, sistemas, equipamentos e demais recursos tecnológicos da universidade. O objetivo é fortalecer os processos de controle de acesso e diminuir os riscos ligados a incidentes cibernéticos, acessos indevidos e vazamento de dados institucionais. De acordo com o diretor do CTIC, Diogo Soares Moreira, a Resolução normatiza o uso dos recursos de TI, em conformidade com as políticas da Ufam e do Governo Federal. "Agradecemos os esforços de todos os envolvidos na construção e aplicação desta Resolução e agradecemos também o apoio da comunidade acadêmica rumo a uma Universidade mais segura digitalmente", lembrou.

O que muda?

O diretor explicou que a partir de agora para técnico-administrativos, docentes, terceirizados, estagiários e bolsistas acessarem os e-mails institucionais haverá Autenticação em Dois Fatores (2FA). A dupla autenticação, já em vigor, visa aumentar a proteção das contas institucionais, evitando acessos não autorizados e reforçando a confiança nas comunicações oficiais da Universidade. Para os discentes, o uso do 2FA permanece opcional, embora seja fortemente recomendado como prática de segurança.

3.2. Aprovação da Política de Uso do Serviço de Armazenamento de Dados em Nuvem

Ações:

- Acompanhamento junto ao conselho superior da universidade e providências de correções finais para a publicação da Portaria GR/UFAM n. 56, de 08 de Janeiro de 2026.

- Encaminhamentos registrados no Processo SEI n. 23105.006388/2023-84.



Ministério da Educação
Universidade Federal do Amazonas
Gabinete da Reitora

Boletim de Serviço Eletrônico em 14/01/2026

PORTARIA Nº 56, DE 08 DE JANEIRO DE 2026

O VICE-REITOR DA UNIVERSIDADE FEDERAL DO AMAZONAS, no exercício do cargo de Reitor, usando das competências que lhe confere o Estatuto da Universidade Federal do Amazonas, e

CONSIDERANDO o Inciso I do Artigo 21 do Estatuto da Universidade Federal do Amazonas;

CONSIDERANDO as competências do Conselho de Administração – CONSAD, previstas no Art. 15 do Estatuto da UFAM;

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

CONSIDERANDO a Instrução Normativa Nº 1/2019, de 04 de abril de 2019, da SGD/ME, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISF do Poder Executivo Federal, alterada pelas Instruções Normativas Nº 202/2019/SGD/ME, Nº 31/2021/SGD/ME e Nº 47/2022/SGD;

CONSIDERANDO a Instrução Normativa GSIPR Nº 5/2021, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da Administração Pública Federal;

CONSIDERANDO a Portaria Nº 1600/2020, de 11 de novembro de 2020, que instituiu o Comitê de Governança Digital – CGD no âmbito da Universidade Federal do Amazonas – UFAM, órgão de natureza deliberativa e de caráter estratégico, e demais alterações, conforme Processo SEI nº 23105.000078/2019-70;

CONSIDERANDO o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC/UFAM;

CONSIDERANDO a Política de Segurança da Informação e Comunicações da Universidade Federal do Amazonas, conforme Resolução Nº 04/2024, de 03 de abril de 2024, Conselho Universitário;

CONSIDERANDO a Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação e Comunicação, conforme Resolução Nº 14/2025, de 22 de setembro de 2025, do Conselho Universitário;

CONSIDERANDO as instruções dos autos do Processo SEI nº 23105.006388/2023-84,

R E S O L V E:

Art. 1º. INSTITUIR as normas operacionais de caráter executivo e de condutas específicas para o uso do serviço de armazenamento de dados em nuvem dos serviços Google Workspace da Universidade Federal do Amazonas – UFAM, alinhada à Política de Controle de Acesso à Informação e aos Recursos e Serviços de Tecnologia da Informação da UFAM.

4. DISSEMINAÇÃO DA CULTURA EM SEGURANÇA DA INFORMAÇÃO

4.1. Campanha Segurança no Elemento Humano – SEH

Ações:

- Promoção na universidade da campanha “**Segurança no Elemento Humano – SEH**” onde foram trabalhados os temas de **Autenticação, Segurança Aplicada a Redes Sociais, Segurança em Redes, Vazamento de Dados, Phishing e Outros Golpes e Códigos Maliciosos**. Os temas foram elaborados pelas instituições participantes do Colégio de Gestores de TI e Comunicação (CGTIC) das Instituições Federais de Ensino Federal Superior (IFES) vinculadas à Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (Andifes), dentre as quais a Universidade Federal do Amazonas (Ufam).
- Alinhamento com direção CTIC e ASCOM para trazer a campanha desenvolvida pelo Colégio de Gestores de TI e Comunicação (CGTIC) para a universidade.
- Registro da divulgação da campanha em março de 2025 disponível no sítio da universidade:

<https://www.ufam.edu.br/noticias-destaque/6537-rede-nacional-reune-23-instituicoes-federais-de-ensino-em-campanha-sobre-seguranca-da-informacao.html>



Ir para o conteúdo Ir para o menu Ir para a busca Ir para o rodapé

A+ A- PT EN ES ACESSIBILIDADE ALTO CONTRASTE MAPA DO SITE

UFAM UNIVERSIDADE FEDERAL DO AMAZONAS

Assessoria de Comunicação Carta de Serviços ao Usuário Fale Conosco Webmail

PÁGINA INICIAL > NOTÍCIAS DESTAQUE > REDE NACIONAL REÚNE 23 INSTITUIÇÕES FEDERAIS DE ENSINO EM CAMPANHA SOBRE SEGURANÇA DA INFORMAÇÃO

Rede nacional reúne 23 instituições federais de ensino em campanha sobre segurança da informação

Publicado: Quarta, 26 de Março de 2025, 11h50 | Última atualização em Quarta, 26 de Março de 2025, 12h02 | Acessos: 852

Postar Compartilhar WhatsApp

Até junho, serão trabalhados os temas de Autenticação, Segurança Aplicada a Redes Sociais, Segurança em Redes, Vazamento de Dados, Phishing e Outros Golpes e, ainda, Códigos Maliciosos

Neste ano de 2025, a segurança da informação é trabalhada a partir de um Plano de Conscientização cujo projeto foi elaborado pelas instituições participantes do Colégio de Gestores de TI e Comunicação (CGTIC) das Instituições Federais de Ensino Superior (IFES) vinculadas à Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (Andifes), dentre as quais a Universidade Federal do Amazonas (Ufam). A campanha **Segurança no Elemento Humano – SEH** está dividida em dois planos semestrais que incluem um conjunto de ações de conscientização e de mobilização, atuando em torno de uma temática específica a cada mês.

O objetivo da campanha é fortalecer a cultura de segurança da informação entre as 23 universidades parceiras, conscientizando a comunidade acadêmica a respeito da importância de se proteger as informações institucionais. Ao longo do ano, 12 temas prioritários serão tratados por meio de ações específicas, cuja implementação será realizada de forma escalonada a cada semana, com uso de ferramentas como e-mails informativos, divulgação de cards nos perfis da instituição nas mídias sociais, veiculação de áudios e vídeos informativos e conteúdos adicionais.

[Leia aqui o PDF](#) do primeiro Plano Semestral SEH.

“Os materiais construídos colaborativamente servirão para identificar as necessidades de conscientização, definir estratégias de comunicação eficazes e implementar programas de treinamento que promovam a cultura de segurança da informação em todos os níveis das organizações”, explica a página criada para a campanha.

Dois Planos Semestrais

O Plano de Conscientização Semestral compreende os meses de janeiro a junho de 2025, e também pode ser compreendido como um Plano de Comunicação para a campanha. No documento, os primeiros seis temas são trabalhados um em cada mês, conforme esta distribuição: Autenticação (janeiro); Segurança Aplicada a Redes Sociais (fevereiro); Segurança em Redes (março); Vazamento de Dados (abril); Phishing e Outros Golpes (maio); e Códigos Maliciosos (junho).

4.2. Campanha de Conscientização em Privacidade e Segurança da Informação 2025

Ações:

- Promoção da **“Campanha de Conscientização em Privacidade e Segurança da Informação”** promovida por meio da parceria entre a Coordenação de Segurança da Informação (CSEGINFO/CTIC), o Escritório de Proteção de Dados Pessoais

(EPDP) e a Assessoria de Comunicação (ASCOM) e em conformidade com o Programa de Privacidade e Segurança da Informação (PPSI). A campanha ocorreu em comemoração ao **Dia Internacional da Segurança da Informação** (30 de novembro) e abordou sete temas gerais: **Proteção de Dados, Autenticação Forte e Senhas, Prevenção de Vazamento de Dados, Proteção contra Golpes na Internet, Segurança contra Códigos Maliciosos, Trabalho Remoto Seguro e Redes Sociais.**

- Registros do lançamento da campanha de novembro de 2025 disponível no sítio da universidade:
<https://www.ufam.edu.br/noticias/7240-ufam-promove-campanha-de-conscientizacao-sobre-seguranca-da-informacao-e-privacidade-entre-os-dias-24-e-30-de-novembro.html>

The screenshot shows the UFAM (Universidade Federal do Amazonas) website. The header is green with the UFAM logo and navigation links. The main content area has a white background. The article title is 'Ufam promove Campanha de Conscientização sobre Segurança da Informação e Privacidade entre os dias 24 e 30 de novembro'. Below the title, it says 'Acessos: 807'. The article text mentions that the campaign is part of the annual calendar of the institution and marks the International Day of Information Security on November 30. It lists seven themes: Protection of Data, Strong Authentication and Passwords, Prevention of Data Leakage, Protection against Internet Scams, Security against Malicious Codes, Secure Remote Work, and Social Networks. An illustration shows a person sitting on the floor with a laptop, surrounded by icons representing security concepts like a fingerprint, a padlock, and a shield. The text continues to state that the objective is to raise awareness among the university community about the importance of adopting good security practices in digital environments.

4.3. Capacitação de gestores e participantes do Programa de Gestão por Resultado (PGR)

Ações:

- Em 2025, cerca de **75% dos 686 servidores** (entre participantes e gestores) no PGR concluíram **curso de capacitação em Segurança da Informação**, conforme dados fornecidos pela **equipe responsável pelo PGR.**

- Determinação de incorporação do curso “**Segurança da Informação para Todos (24h)**” como requisito obrigatório foi encaminhado pela PROGESP no Processo SEI n. 23105.013742/2025-99 e ocorreu em consequência de **encaminhamentos iniciados pela CSEGINFO** no exercício anterior.
- Referência no site do programa:
<https://progesp.ufam.edu.br/cursos-enap-requisitados-para-o-programas-de-gestao-pgr.html>



4.4. Capacitação do time de servidores da CSEGINFO em cursos, formações, workshops e webinários voltados para segurança da informação

Ações:

Workshops

- Backup: sua última linha de defesa. Instituição: Tribunal de Contas da União / Instituto Serzedello Corrêa. Período: outubro de 2025.
- Pesquisa de preços de TI: Estratégias e Boas Práticas. Instituição: Tribunal de Contas da União / Instituto Serzedello Corrêa. Período: outubro de 2025.

Webinários

- Proteção contra Ransomware. Instituição: CTIR Gov.br. Período: outubro de 2025.
- Análise de Vulnerabilidades e Pentest. Instituição: SOC RNP. Período: novembro de 2025.

- PPSI 2.0. Instituição: Secretaria de Governo Digital / Ministério da Gestão e da Inovação. Período: novembro de 2025
- Da Detecção à Resposta: Ciber Kill Chain e MITRE ATT&CK. Instituição: CEPS Gov.br / CISC [Gov.br](https://gov.br). Período: dezembro de 2025.

Cursos livres

- **Plataforma EaD da RNP:** Cibersegurança, Gestão de Riscos de Segurança da Informação e Privacidade, Tratamento de incidentes de Segurança, Security+, CySA+, PenTest+, SecurityX e LGPD na Prática.
- **Plataforma ENAP:** Fundamentos da Segurança Cibernética – Introdução ao CIS Controls, Segurança Cibernética: Controles 13 a 18 do CIS Controls,
- **Plataforma Alura:** Segurança Defensiva, Segurança Ofensiva, LGPD: Conhecendo a Legislação para Proteger Dados Pessoais,