MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA
REITORIA
Comitê de Governança Digital

ATA DA 1ª REUNIÃO ORDINÁRIA DO COMITÊ DE COMITÊ DE GOVERNANÇA DIGITAL (CGD) E DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI) DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA – IFRR, REALIZADA EM 09 DE MARÇO DE DOIS MIL E VINTE E SEIS.

REUNIÃO CONJUNTA DOS COMITÊS
Comitê de Governança Digital (CGD), Comitê Gestor de Segurança da Informação (CGSI) e Comitê de Governança, Gestão de Riscos e Controles Internos (CGOV)

1. ABERTURA DA SESSÃO
Aos nove dias do mês de março do ano de dois mil e vinte e seis, às quatorze horas e trinta minutos, no formato presencial, reuniu-se Comitê de Comitê De Governança Digital (CGD) E Do Comitê Gestor De Segurança Da Informação (CGSI) e o o Comitê de Governança, Gestão de Riscos e Controles Internos (CGOV).

1.1 Verificação do quórum: Estavam presentes os seguintes representantes do Comitê de Governança, Gestão de Riscos e Controles Internos: Aline Cavalcante Ferreira, Diogo Rocha Ferreira Maia, Emanuel Alves de Moura, Rafaela dos Santos Morgade representando o Diretor-Geral do Campus Boa Vista Zona Oeste, Luciana Leandro Silva, Adnelson Jati Batista, Amarildo Ferreira Júnior representando o Pró-reitor de Pesquisa, Pós-graduação e Inovação, Rodrigo Luiz Neves Barros, Roseli Bernardo Silva dos Santos, Tomaz Armando Del Pozo Hernandez e Vanessa Rufino Vale Vasconcelos. Estavam presentes também: Adriene Silva do Nascimento, Jonatas Silva Lima, Antônia Valdirene Rabelo Costa, Fábio Rodrigues dos Santos, Ivania Nascimento Ferreira Carvalho, Jorgehanny Barroso Tocantins e Érika Patrícia Batista Pereira. Havendo quórum suficiente, iniciou-se a reunião.

1.2 Abertura da Reunião: A Presidente em exercício, Aline Cavalcante Ferreira, realizou a abertura, da pauta da reunião e passou a palavra ao Diretor de Tecnologia e Informação, O diretor de Tecnologia e Informação da DTI, Diogo Maia apresentou a pauta da reunião para os presentes enviada por e-mail anteriormente. conforme o regimento do comitê, que justificam as pautas da presente reunião.

2. ORDEM DO DIA:

2.1 Migração para Nuvem de Governo (SERPRO Multicloud)

O Diretor de Tecnologia da Informação (DTI), Diogo Maia, apresentou o projeto de contratação de infraestrutura em nuvem, destacando a migração de serviços críticos — como SUAP, SGC, repositório, autenticação de usuários, Rapsign e o portal institucional — para o ambiente **Multicloud do SERPRO**. A urgência da medida foi justificada pelas frequentes instabilidades no acesso aos sistemas, decorrentes de falhas de conectividade do provedor.

O Diretor ratificou os riscos institucionais vigentes, pontuando que os equipamentos do *datacenter* local atingiram o fim do ciclo de vida, encontrando-se sem garantia ou suporte técnico, o que impossibilita a renovação de licenças. Ressaltou que, embora a migração para a nuvem seja uma estratégia vital de mitigação de riscos, permanece a necessidade de renovar a infraestrutura local para suportar os sistemas que, por limitações orçamentárias do contrato de nuvem, não serão migrados.

Na sequência, foram apresentados os custos orçados pelo SERPRO para a elaboração da arquitetura de solução dos serviços de autenticação e do SUAP. O Diretor informou que autorizou a execução do projeto de arquitetura do serviço de autenticação; contudo, devido ao alto valor demandado para o desenho da arquitetura do SUAP, a execução deste último

não foi autorizada junto à referida empresa.

Sobre esse ponto, destacou-se a atuação técnica interna: o analista da DTI, Francisco, dedicou semanas ao estudo da documentação da AWS (provedor de nuvem) para a implantação do serviço de autenticação (**Active Directory**), que já se encontra em produção. **Ressaltou-se, ainda, a importante colaboração do analista de TIC Fábio Rodrigues no desenho da arquitetura dos serviços em nuvem**, garantindo a viabilidade técnica da solução.

A migração deste serviço resultou em ganho de qualidade para o Ambiente Virtual de Aprendizagem (AVA), devido à comunicação direta entre ambientes de nuvem e à tecnologia de alta disponibilidade. **Essa iniciativa gerou uma economia estimada de R$ 150.000,00 (cento e cinquenta mil reais)** à instituição. O Diretor aproveitou a oportunidade para reforçar que o investimento na equipe de TIC é essencial para gerar economias em diversas contratações.

Por fim, o Diretor explicou a criação de um grupo de trabalho composto por quatro analistas e um técnico de TI. O objetivo é promover a transferência de conhecimento sobre tecnologia em nuvem, descentralizando o saber técnico e mitigando riscos à continuidade dos serviços de TIC, evitando que a instituição dependa exclusivamente de um único servidor.

2.2 Novo Módulo SUAP + CKAN (Dados Abertos):

Informou-se ao comitê que, durante a atualização do **SUAP** realizada em novembro de 2025, foi identificada a disponibilização de um novo módulo de **Dados Abertos** desenvolvido pelo IFRN. Este módulo permite a integração direta com o **CKAN**, funcionando como uma ponte automatizada para o portal de transparência institucional e facilitando o acesso da comunidade a dados estruturados e legíveis por máquina.

Contudo, ressaltou-se que, apesar da disponibilidade técnica da ferramenta, a configuração e abertura das bases de dados dependem da criação de uma comissão para a atualização do **Plano de Dados Abertos (PDA)**, uma vez que o documento anterior expirou em 2023. Somente após a vigência de um novo plano será possível configurar o módulo para publicar as bases de dados previstas. No âmbito da **Transparência Ativa**, o foco inicial dessa implementação será a disponibilização de dados orçamentários (e outros dados previstos em PDA vigente) em formatos abertos (CSV, XLSX e JSON), garantindo que a instituição esteja em plena conformidade com a **Lei de Dados Abertos**.

A servidora Adriene Silva do Nascimento reforçou a necessidade estratégica dessa atualização do PDA, enfatizando que o aprimoramento do instrumento é fundamental para melhorar — ou consolidar — o ranqueamento da instituição junto aos órgãos de controle, como a Controladoria-Geral da União (**CGU**). Destacou, ainda, a importância de alinhar o PDA ao **Plano de Desenvolvimento Institucional (PDI)**, conectando as ferramentas de transparência ativa aos indicadores de desempenho exigidos pela administração pública federal.

2.3 Encaminhamentos do Item 2.2:

Ficou deliberada a constituição imediata da Comissão de Dados Abertos, bem como a designação da Autoridade de Monitoramento da LAI para a supervisão das atividades. Adicionalmente, definiu-se a indicação de um analista da CDSS para garantir a configuração e integração técnica entre os sistemas (SUAP e CKAN), assegurando o cumprimento dos requisitos de transparência ativa de forma automática.

3. Comitê Gestor de Segurança da Informação (CGSI)

Dando continuidade à pauta, **Fabio Santos,** Gestor de Segurança e Informação - GSI e presidente do Comitê de SI, apresentou o **Programa de Privacidade e Segurança da Informação (PPSI)**. Informou que a iniciativa é coordenada pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) e visa orientar órgãos públicos na adoção de práticas de segurança e proteção de dados, integrando o diagnóstico de conformidade ao controle da informação.

Fabio Santos iniciou falando sobre o PPSI, que está atualmente na versão 2.0, e falou sobre as funções do Encarregado de Dados, com base na Lei Geral de Proteção de Dados (LGPD), e explicou que a segurança da informação está relacionada aos equipamentos e estruturas de segurança. Informou que o IFRR precisa entregar um Relatório Diagnóstico, que é feito por meio de um preenchimento de um framework. Fabio informou que antes ele fazia esse preenchimento sozinho, mas que agora, foi dividido em 3 partes, pois o MGI e TCU estão procurando por evidências da participação da alta administração na segurança da informação. Eles estabeleceram que a alta administração deve fazer a gestão de riscos da segurança da informação. É necessário também enviar um Plano de Trabalho, mas primeiro é preciso realizar a gestão de riscos para detectar o que deve ser priorizado. Fabio Santos explicou que a segurança da informação não é uma dimensão estratégica, mas que perpassa por todas as dimensões (é transversal). Apresentou o cadastro dos gestores e substitutos que foi feito no framework, e os demais itens que já foram preenchidos e quais ainda estão pendentes. Fabio Santos finalizou informando que devido à falta da implementação da gestão de riscos em segurança da informação, o IFRR está ainda no nível inicial de maturidade na estrutura básica para a governança, e frisou sobre a responsabilidade do CGOV em realizar a gestão de riscos em segurança da informação.

Foi destacado que o **PPSI 2.0** introduz novas diretrizes de governança e ferramentas de diagnóstico essenciais, fundamentadas em um *framework* de ciclos e guias práticos, com ênfase no **Controle Zero** para a gestão básica de segurança. No âmbito operacional, o programa prioriza medidas críticas, o fortalecimento da cultura de segurança e a interoperabilidade segura, sendo de aplicação obrigatória para instituições públicas federais membros do SISP.

Auditorias: Alinhamento sobre recomendações do TCU e Auditoria Interna em LGPD (Acórdão).

Fabio ressaltou que a SGD/MGI disponibilizou uma planilha para o preenchimento do diagnóstico com acesso otimizado. Explicou que, após a aprovação deste diagnóstico, seguem-se as etapas do **Plano de Trabalho** e a entrega. Informou, ainda, que a instituição já conta com um Encarregado de Dados (DPO) e seu respectivo substituto, além de atores como o **Gestor de Integridade/Degov** na interlocução com o MGI. Pontuou que, anteriormente, não havia uma estruturação básica de governança, o que reflete o atual **Índice 1 nos controles base**.

Na oportunidade, o Presidente do CGSI apresentou o fluxo do macroprocesso de **Gestão de Riscos**, notando, porém, a ausência de capacitação em gestão por parte dos gestores. Complementando a exposição, o senhor **Fabio**, Item 1.2 "*Desenvolvimento Contínuo dos Agentes Públicos em Gestão de Riscos Haja vista a inexperiência institucional sobre gestão de riscos, a instituição deverá contemplar, no seu plano de capacitação, a oferta/participação em capacitação sobre o tema pelo menos aos membros do Comitê de Governança, Gestão de Riscos e Controles Internos, que, posteriormente, deverão replicar os conhecimentos adquiridos às demais partes envolvidas no processo*", presente no Manual de Gestão de do IFRR de 2020. Ao perguntar aos presentes, membros do referido comitê, se tinham realizado capacitação em gestão de riscos, obteve resposta negativa. Passando em seguida a apresentar os instrumentos e ferramentas de gestão de riscos aplicadas aos processos ligados a privacidade e segurança da informação que estão sendo cobrados pelos órgãos de controle.

3.1 Encaminhamentos:

- A alta administração deve estabelecer, manter, monitorar e aprimorar o sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica dos riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional (Decreto nº 9203/2017, art. 17), sem prejuízo das responsabilidades dos gestores dos processos organizacionais. Nesse contexto, os temas de privacidade e segurança da informação devem estar integrados ao sistema de gestão de riscos e aos controles internos. Ademais, conforme Acórdão 2387/2024 – Plenário TCU, a alta administração da organização deve liderar o processo de gestão de riscos decorrentes de ataques cibernético.
- Instituir e implementar, preferencialmente em instância colegiada, o PGSI, documento que contém, no mínimo, o disposto na IN GSI/PR nº 3/2021, art. 45, na forma de ações estruturadas, políticas, normas e procedimentos para promover a segurança da informação na organização. Recomenda-se que o PGSI contemple papéis e responsabilidades dos agentes públicos envolvidos em sua execução, os prazos para realização das ações, além da programação para implementação dos controles e medidas de segurança da informação do PPSI, e que especifique indicadores de desempenho, como o iSeg, a serem medidos ao longo da execução do Programa. Revisar e atualizar o PGSI com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas de suas ações.
- Instituir e implementar, preferencialmente em instância colegiada, o PGP, documento que contém, no mínimo, o disposto na Lei nº 13.709/2018, art. 50, §2°, I, na forma de ações estruturadas, políticas, normas e procedimentos para o tratamento de dados pessoais pela organização. Recomenda-se que o PGP contemple papéis e responsabilidades dos agentes públicos envolvidos em sua execução, os prazos para realização das ações, além da programação para implementação dos controles e medidas de privacidade e proteção de dados pessoais do PPSI, e que especifique indicadores de desempenho, como o iPriv, a serem medidos ao longo da execução do Programa. Revisar e atualizar o PGP com base em informações obtidas a partir de monitoramento contuíno e avaliações periódicas de suas ações.
- Estabelecer e manter, em conformidade ao Capítulo III da IN GSI/PR nº 3/2021, um processo de gestão de riscos de segurança da informação alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos da organização considerando o disposto nos incisos do art. 11. Além disso, o processo deve ser composto por, no mínimo: plano de gestão de riscos de segurança da informação, conforme disposto no art. 13; relatório de identificação, análise e avaliação dos riscos de segurança da informação, conforme disposto no art. 14; e, relatório de tratamento de riscos de segurança da informação, conforme disposto no art. 15. Considerar as atribuições dispostas nos arts. 16 e 17.
- Estabelecer e manter, em conformidade ao Capítulo IV da IN GSI/PR nº 3/2021, um processo de gestão de continuidade de negócios em segurança da informação baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e nas diretrizes institucionais sobre gestão de continuidade de negócio. Tal processo deve ser composto por um plano de continuidade de negócios em segurança da informação, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio, revisado uma vez por ano ou

após mudanças significativas nos itens que compõem o plano. Além disso, o conteúdo do plano deve incluir o disposto no art. 23, e ser testado regularmente. Considerar as atribuições dispostas nos arts. 25, 26 e 27.

4.. Encerramento da Reunião e às 16h10.

Nada mais havendo a tratar, a Presidência encerrou a reunião às 16h10, agradecendo a todos.

5. Registro da Ata

Eu, Ivânia Nascimento Ferreira Carvalho, Secretária dos Comitês CGD e CGSI, lavrei a presente ata, que será assinada eletronicamente após aprovação e publicada no site oficial do IFRR.

6. MEMBROS E REPRESENTANTES DO CGOV

- Aline Cavalcante Ferreira (Pró-reitora de Ensino; representando Presidente do CGD - Reitora Nilra Jane Filgueira Bezerra)
- Amarildo Ferreira Júnior (representando Pró-reitor de Pesquisa)
- Adnelson José Rossetti Junior (Pró-reitor de Desenvolvimento Institucional)
- Diogo Rocha Ferreira Maia (Diretor de Tecnologia da Informação - DTI)
- Fábio Rodrigues dos Santos (Presidente do CGSI)
- Emanuel Alves de Moura (Pró-reitor de Administração)
- Luciana Leandro Silva (Diretora-Geral do Campus Boa Vista)
- Rafaela dos Santos Morgade (representando Diretor-Geral do Campus Boa Vista Zona Oeste)
- Rodrigo Luiz Neves Barros (Diretor-Geral do Campus Amajari)
- Roseli Bernardo Silva dos Santos (Pró-reitora de Extensão)
- Tomaz Armando Del Pozo Hernandez (Diretor-Geral do Campus Avançado Bonfim)
- Vanessa Rufino Vale Vasconcelos (Diretora-Geral do Campus Novo Paraíso)

7. REPRESENTANTES DAS INSTÂNCIAS INTERNAS E CONVIDADOS

- Adriene Silva do Nascimento (1455212)
- Jonatas Silva Lima (2109643)
- Antônia Valdirene Rabelo Costa (2108788) convidada
- Érika Patrícia Batista Pereira (1118797) convidada
- Jorgehanny Barroso Tocantins (1792758) convidada

Secretária da Reunião: Ivânia Nascimento Ferreira Carvalho (709212)

Documento assinado eletronicamente por:

- **Adriene Silva do Nascimento**, **DIRETOR(A) DE DEPARTAMENTO - CD0004 - DEGOV**, em 30/03/2026 08:37:25.
- **Antonia Valdirene Rabelo Costa**, **COORDENADOR(A) - FG0004 - COAPE**, em 31/03/2026 09:42:09.
- **Ivania Nascimento Ferreira Carvalho**, **AUX EM ADMINISTRACAO**, em 31/03/2026 09:51:08.
- **Aline Cavalcante Ferreira**, **PRO-REITOR(A) - CD0002 - PROEN**, em 26/03/2026 11:47:51.
- **Vanessa Rufino Vale Vasconcelos**, **DIRETOR(A) GERAL - CD0002 - DG-CNP (CNP)**, em 26/03/2026 12:02:11.
- **Erika Patricia Batista Pereira**, **COORDENADOR(A) - FG0004 - CTI (CNP)**, em 26/03/2026 12:04:43.
- **Amarildo Ferreira Junior**, **PRO-REITOR(A) - SUB-CHEFIA - PROPESPI**, em 31/03/2026 10:24:15.
- **Rodrigo Luiz Neves Barros**, **DIRETOR(A) GERAL - CD0002 - DG-CAM (CAM)**, em 26/03/2026 15:40:46.
- **Luciana Leandro Silva**, **DIRETOR(A) GERAL - CD0002 - DG-CBV (CBV)**, em 26/03/2026 18:08:18.
- **Diogo Rocha Ferreira Maia**, **DIRETOR(A) - CD0003 - DTI**, em 26/03/2026 18:13:11.
- **Roseli Bernardo Silva dos Santos**, **PRO-REITOR(A) - CD0002 - PROEX**, em 27/03/2026 10:35:06.
- **Fabio Rodrigues dos Santos**, **ANALISTA DE TEC DA INFORMACAO**, em 27/03/2026 12:58:49.
- **Emanuel Alves de Moura**, **PRO-REITOR(A) - CD0002 - PROAD**, em 26/03/2026 11:58:25.
- **Jorgehanny Barroso Tocantins**, **ADMINISTRADOR**, em 27/03/2026 10:43:52.
- **Jonatas Silva Lima**, **AUDITOR(A) - FG0001 - AUDIN**, em 27/03/2026 10:23:07.
- **Rafaela dos Santos Morgade**, **SUB-CHEFIA - DG-CBVZO (CBVZO)**, em 27/03/2026 10:39:19.
- **Tomas Armando del Pozo Hernandez**, **DIRETOR(A) GERAL - CD0002 - DICAB (CAB)**, em 01/04/2026 10:59:58.
- **Adnelson Jati Batista**, **PRO-REITOR(A) - CD0002 - PRODIN**, em 27/03/2026 14:50:20.
