MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

RESOLUÇÃO Nº 09, DE 21 DE MAIO DE 2025

Institui a Estratégia do uso de software e de serviços de computação em nuvem para a UFVJM

O COMITÊ DE GOVERNANÇA INTEGRIDADE, RISCOS E CONTROLE DA UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI, no uso das atribuições legais e regulamentares, tendo em vista o que consta do processo 23086.047529/2024-75 e o que fora deliberado na 46 ª reunião, resolve:

Art. 1º Instituir a Estratégia do uso de software e de serviços de computação em nuvem para a UFVJM.

Art. 2º O referido Plano encontra-se anexo a presente Resolução.

Art. 3º Esta Resolução entrará em vigor na data de sua assinatura.

HERON LAIBER BONADIMAN

Presidente CGIRC

Documento assinado eletronicamente por **Heron Laiber Bonadiman**, **Reitor**, em 21/05/2025, às 11:30, conforme horário oficial de Brasília, 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.ufvjm.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1767722** e o código CRC **736B7125**.

ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM PARA A UFVJM

I-DISPOSIÇÕES GERAIS

O presente documento apresenta diretrizes para nortear a UFVJM no processo de modernização da sua infraestrutura tecnológica para suportar softwares e outras soluções de tecnologia da informação e comunicação (TIC). Busca-se uma modernização da infraestrutura tecnológica da UFVJM nesse aspecto, a partir da migração para soluções mais flexíveis e seguras, com melhor custo-benefício e alinhamento com as práticas atuais de gestão pública digital do Governo Federal.

II-OBJETIVOS E COMPETÊNCIAS

2.1 A adoção da presente Estratégia tem principalmente os seguintes objetivos:

2.1.1. Modernizar a Infraestrutura de TIC da UFVJM, possibilitando a atualização tecnológica de sistemas e serviços providos pela Superintendência de Tecnologia da Informação (STI). Atualmente a maioria dos sistemas se encontra hospedada em um data center local no campus JK, com equipamentos e as respectivas licenças relacionadas aos mesmos já obsoletas. A modernização se dará para um ambiente de computação em nuvem, garantindo maior flexibilidade, escalabilidade e continuidade operacional.

2.1.2. Garantir a disponibilidade dos serviços e a recuperação de dados, a partir da implementação de soluções de backup e recuperação de desastres. Isso elimina a atual limitação da falta de um *site backup* e assegura que os serviços essenciais continuem operacionais, mesmo em caso de falhas no data center.

2.1.3. Melhorar a gestão da segurança da informação, através da adoção de medidas contra ameaças cibernéticas para proteção dos dados produzidos e sob guarda da UFVJM. Tal medida auxilia no atendimento aos requisitos da Lei Geral de Proteção de Dados (LGPD) e demais normas de segurança aplicáveis à realidade da UFVJM.

2.1.4. Otimizar os custos com soluções de TIC, possibilitada por meio da redução dos custos tanto com manutenção de infraestrutura física de TI, como da renovação do parque tecnológico. A redução será possível por meio da adoção de modelos de serviços em nuvem computacional sob demanda, os quais geram gasto apenas conforme o efetivo uso dos recursos.

2.1.5. Facilitar o acesso a novas tecnologias, as quais se encontram disponíveis pelos principais provedores de computação em nuvem, sendo constantemente atualizadas na medida em que novas soluções são geradas. O acesso a serviços inovadores e tecnologias emergentes disponíveis em ambientes de nuvem, como orquestração de contêineres, inteligência artificial, aprendizado de máquina e análise de big data, podem ser utilizados no apoio a atividades acadêmicas e administrativas.

2.2 Em relação às competências a serem desenvolvidas, pode-se destacar:

2.2.1. Gestão de Serviços em Nuvem: desenvolver a capacidade interna da equipe da UFVJM de planejar, contratar e gerir serviços de computação em nuvem, incluindo a análise de custo-benefício e a gestão de contratos com os fornecedores.

2.2.2. Gestão de Segurança da Informação: implementar competências específicas para a proteção de dados em ambientes de nuvem, incluindo práticas de governança, conformidade regulatória e gestão de riscos.

2.2.3. Gestão de Mudanças Organizacionais: habilitar a UFVJM a lidar com as mudanças associadas à migração para a nuvem, incluindo a capacitação de pessoal, adaptação de processos e gestão da transição dos serviços da estrutura local (*on-premises*) para a nuvem.

2.2.4. Gestão de Custos Operacionais: possibilitar que os gastos em nuvem sejam previsíveis, controlados e otimizados. Para tanto, faz-se preciso o acompanhamento contínuo de como os recursos computacionais estão sendo consumidos, bem como o custo financeiro associado.

2.2.5. Gestão de Continuidade de Negócio e Recuperação de Desastres: desenvolver a capacidade de planejar e executar estratégias de recuperação de desastres, assegurando que os dados e serviços críticos possam ser rapidamente restaurados em situações de crise.

III-DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

A seguir são apresentados os aspectos que foram considerados na definição, no âmbito da UFVJM, das diretrizes da estratégia para o uso de software e de serviços de computação em nuvem:

3.1.1 Sistemas a Serem Migrados ou Mantidos em Nuvem

Para a UFVJM modernizar seus sistemas, melhorar eficiência operacional e garantir uma infraestrutura tecnológica segura e resiliente, é necessária e migração dos seguintes tipos de dados e serviços:

3.1.1.1 Dados e sistemas acadêmicos e administrativos: Dados relacionados ao registro de alunos, matrículas, históricos escolares, gestão de cursos, bibliotecas, repositórios acadêmicos e plataformas de ensino. Também processos administrativos, como gestão de aquisições, contratos, bens móveis e imóveis, assim como gestão de recursos humanos. Isso garante a disponibilidade em caso de falhas no data center local e facilita, portanto, o acesso remoto.

3.1.1.2. Sistemas de Comunicação e Colaboração: Serviço de e-mail, ferramentas de colaboração e plataforma de videoconferência.

3.1.1.3. Serviços de Backup e Recuperação de Desastres: Soluções para aplicação da política de *backup* e retenção dos dados, assim como das ferramentas para recuperação de desastres.

3.1.1.4. Sistemas e Ferramentas para Desenvolvimento de Software: Ambientes, ferramentas e plataformas para desenvolvimento e testes de soluções de tecnologia da informação.

3.1.2 Lista de Sistemas a Serem Movidos para Nuvem

A lista de sistemas a serem migrados para a nuvem, ou mesmo aqueles que já se encontram em nuvem pública, encontra-se discriminada no Anexo I dessa resolução.

3.1.3 Acesso aos Recursos e Sistemas

De modo a cumprir as boas práticas e a legislação relacionada à segurança da informação e privacidade de dados, o acesso aos recursos e sistemas devem seguir os seguinte princípios e procedimentos:

3.1.3.1. Acesso controlado, com estabelecimento da política de controle de acesso baseado em papéis, além de mecanismos de autenticação baseados em múltiplos fatores.

3.1.3.2. Monitoramento e registro de atividades, com a implementação do serviço de gestão de logs para acompanhar tanto o emprego de recursos como o registro de atividades executadas.

3.1.3.3. Alta disponibilidade dos serviços e dados, através de soluções implementadas por redundância geográfica ou mesmo de redes de entrega de conteúdo (CDN).

3.1.3.4. Recursos computacionais sob demanda, com o emprego de máquinas virtuais escaláveis ou serviços de contêineres para gerenciar cargas de trabalho dinâmicas. Isso permitirá a alocação de recursos computacionais conforme a demanda, evitando sobrecargas e garantindo o desempenho.

3.2 Seleção dos Modelos Adequados

3.2.1 Modelos de Serviço a Serem Implementados: para atender às diferentes demandas por soluções de TIC na UFVJM, será necessário utilizar os três modelos de serviços em nuvem (Infraestrutura como Serviço, Plataforma como Serviço e Software como Serviço).

Cada modelo oferece benefícios específicos que são essenciais para atender às necessidades diversas da universidade, conforme explicado a seguir:

3.2.1.1. IaaS (Infraestrutura como Serviço): necessário para a migração de cargas de trabalho que demandam controle completo sobre a infraestrutura, como a criação de máquinas virtuais para hospedar sistemas acadêmicos e administrativos críticos. O uso de IaaS permitirá escalar recursos de computação e armazenamento de acordo com as necessidades, reduzindo a dependência de infraestrutura física obsoleta.

3.2.1.2. PaaS (Plataforma como Serviço): Facilitará o desenvolvimento e a implantação de aplicações personalizadas, especialmente para sistemas de ensino, repositórios de dados de pesquisa e portais institucionais. O PaaS oferece ambientes de desenvolvimento e bancos de dados gerenciados, agilizando a entrega de novas funcionalidades e reduzindo a complexidade da gestão de infraestrutura.

3.2.1.3. SaaS (Software como Serviço): Ideal para sistemas padronizados e de uso comum, como e-mail institucional, plataformas de colaboração e gestão de documentos. O SaaS proporciona fácil acesso a soluções prontas para uso, diminuindo a necessidade de manutenção e atualizações por parte da equipe interna de TI.

A utilização combinada dos três modelos permitirá a flexibilização da infraestrutura de TI da UFVJM, promovendo eficiência e adaptabilidade para diversas aplicações e necessidades institucionais.

3.2.2 Modelos de Implementação de Nuvem

A adoção de uma abordagem de nuvem híbrida, com predomínio da nuvem pública para a maior parte das cargas de trabalho, é a estratégia mais adequada para a UFVJM, levando em consideração os seguintes fatores:

3.2.2.1. Compatibilidade com Sistemas Locais: alguns sistemas, como serviços de rede interna, ou aplicações que requerem baixa latência local, como serviço de LDAP, não são vantajosos para migração completa para a nuvem pública. A manutenção desses serviços

em infraestrutura local permitirá um melhor desempenho e controle para alguns tipos de serviço.

3.2.2.2. Gerenciamento de Logs e Alta Carga de Dados: sistemas que geram um grande volume de logs ou dados operacionais, como sistemas de monitoramento de segurança de rede e circuito de câmeras (CFTV), podem não ser compensatórios para operar exclusivamente na nuvem pública devido aos custos de transferência e armazenamento. O uso de uma solução híbrida permite que esses dados sejam armazenados e processados localmente, com a possibilidade de backup na nuvem pública para fins de segurança.

3.2.2.3. Escalabilidade e Custo-Benefício da Nuvem Pública: para a maioria dos sistemas acadêmicos e administrativos, a nuvem pública oferece escalabilidade e custo-benefício superiores, especialmente em termos de elasticidade para lidar com picos de demanda (como períodos de matrícula). A nuvem pública elimina a necessidade de investimento em infraestrutura física, permitindo o pagamento apenas pelos recursos efetivamente utilizados.

3.2.2.4. Segurança e Continuidade de Serviços: uma abordagem híbrida garante maior flexibilidade em termos de segurança. Serviços e dados críticos podem ter cópias e instâncias mantidas em uma estrutura local além de operarem em nuvem pública, garantindo resiliência e continuidade dos serviços.

3.3 Avaliação de Fornecedores Disponíveis

Embora existam opções limitadas de grandes provedores de nuvem, a capacidade de atender aos requisitos de segurança, conformidade, disponibilidade e suporte técnico justifica a seleção de um conjunto de fornecedores para serviços de computação em nuvem na UFVJM. Essa abordagem garante que a universidade tenha acesso a serviços de alta qualidade e suporte adequado para a modernização da sua infraestrutura de TI.

Existe uma quantidade suficiente de fornecedores de soluções de *cloud computing* no Brasil que são capazes de atender aos requisitos do negócio e legais necessários à UFVJM, pelos seguintes aspectos:

3.3.1. Disponibilidade e segurança: no território brasileiro, existe uma quantidade limitada de grandes provedores de serviços de computação em nuvem com infraestrutura robusta e

capacidade de atender aos requisitos de segurança e disponibilidade. Provedores como Amazon Web Services (AWS), Microsoft Azure e Google Cloud, que aparecem consistentemente no quadrante do Gartner como líderes em infraestrutura de nuvem, possuem data centers em várias regiões do mundo, incluindo o Brasil. Isso garante conformidade com leis e regulamentos locais, além de minimizar a latência no acesso aos serviços.

Esses provedores oferecem alta disponibilidade e possuem mecanismos de redundância que garantem a continuidade dos serviços, mesmo em caso de falhas. Além disso, a segurança é uma prioridade, com controles avançados que atendem a normas internacionais e locais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

3.3.2. Conformidade com Normas e Regulamentações: os principais fornecedores de nuvem possuem certificações e atendem a requisitos de conformidade que são fundamentais para o uso institucional, especialmente para organizações públicas. AWS, Azure e Google Cloud, por exemplo, são certificados com normas como ISO/IEC 27001 (Gestão de Segurança da Informação), SOC 2 e PCI-DSS, o que garante que os dados sejam geridos de forma segura e conforme as regulamentações. Essa conformidade é crucial para organizações como a UFVJM, que precisa assegurar a proteção de dados acadêmicos e administrativos.

3.3.1.3. Rede de Suporte Técnico e Parceiros: esses grandes provedores possuem ampla rede de parceiros e suporte técnico no Brasil, incluindo representantes locais e *cloud brokers* que ajudam a implementar, gerenciar e otimizar soluções em nuvem. A presença de parceiros qualificados e uma rede de suporte local garantem que as demandas de manutenção, configuração e suporte sejam atendidas com rapidez e eficiência.

3.3.4. Principais Provedores e Parcerias no Brasil: de acordo com o Quadrante Mágico do Gartner para Infraestrutura de Nuvem, AWS, Microsoft Azure e Google Cloud são os principais líderes. No Brasil, esses provedores têm presença consolidada, com data centers em regiões como São Paulo e parcerias com várias empresas locais que atuam como integradores e prestadores de serviços complementares. Essa infraestrutura e rede de

parceiros garantem que as soluções possam ser adaptadas e escaladas de acordo com as necessidades específicas da UFVJM.

3.4 Definição De Requisitos De Segurança

Abaixo se encontram os requisitos de segurança mais importantes para serem considerados na implantação do ambiente de computação em nuvem pública para os sistemas da UFVJM. Concomitantemente, também são mencionados os recursos disponíveis nos principais provedores que atendem aos citados requisitos:

3.4.1 Criptografia de Dados tanto em Trânsito como em Repouso: para proteção dos dados sensíveis contra acessos não autorizados, tanto enquanto eles estão armazenados quanto durante sua transmissão pela rede.

- **Conformidade dos Provedores**: AWS, Microsoft Azure e Google Cloud oferecem criptografia robusta usando padrões como AES-256 para dados em repouso e TLS para dados em trânsito, assegurando que os dados da UFVJM estejam protegidos em todas as etapas de armazenamento e transmissão

3.4.2 Autenticação Multifator (AMF) e Controle de Acessos Baseado em Papéis (CABP): A AMF adiciona uma camada extra de segurança para se prover o acesso aos sistemas. O CABP, por sua vez, garante que os usuários tenham permissões apropriadas com base em suas funções e apenas naquilo que for necessário para execução dessas funções.

- Conformidade dos Provedores: Todos os principais provedores oferecem AMF e suporte para CABP. A AWS, por exemplo, tem o IAM (*Identity and Access Management*), enquanto o Azure usa o *Azure Active Directory* para controle segmentado de acesso. Isso permite à UFVJM restringir o acesso com alta precisão e segurança.

3.4.3 Atendimento às Regulamentações de Privacidade e Segurança: baseia-se na conformidade com normas como a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações globais de segurança, as quais procuram garantir a proteção de dados pessoais e minimizam os riscos de multas e sanções.

- Conformidade dos Provedores: AWS, Azure e Google Cloud possibilitam o atendimento a normas internacionais como ISO 27001, SOC 2, PCI-DSS, como também normas locais (LGPD), disponibilizando certificações que comprovam a aderência a essas regulamentações. Isso garante que os dados da UFVJM sejam geridos dentro das práticas mais adequadas de proteção e privacidade.

3.4.4 Monitoramento Contínuo e Detecção de Ameaças: o monitoramento contínuo permite a detecção proativa de atividades suspeitas e facilita a resposta a incidentes, o que minimiza o impacto de possíveis violações de segurança dos sistemas.

- Conformidade dos Provedores: esses provedores oferecem ferramentas de monitoramento e análise de ameaças. Por exemplo, o AWS GuardDuty e o Azure Security Center identificam padrões anômalos e notificam sobre atividades suspeitas em tempo real, o que assegura que os ambientes da UFVJM estejam sob vigilância contínua.

3.4.5 Resiliência e Recuperação de Desastres: é crucial haver um plano para recuperação de desastres. E deve haver ferramentas suficientes para possibilitar a execução dos procedimentos previstos no plano. Isso possibilita que dados e serviços possam ser restaurados rapidamente após incidentes de segurança ou falhas de sistema.

- Conformidade dos Provedores: AWS, Azure e Google Cloud oferecem opções robustas de recuperação de desastres, como replicação geográfica e backups automáticos. A AWS, por exemplo, fornece soluções de backup e recuperação com configurações de *failover*, o que é essencial para a continuidade dos serviços críticos da UFVJM.

3.4.6 Gerenciamento de Auditoria: o gerenciamento de logs de atividades no ambiente de nuvem ajuda a rastrear atividades e responder a incidentes de segurança, além de atender a requisitos de conformidade.

- Conformidade dos Provedores: todos os principais provedores oferecem gerenciamento de logs centralizado (AWS CloudTrail, Azure Monitor e Google Cloud Audit Logs), que registra as atividades dos usuários e alertas de segurança,

ajudando a UFVJM a manter um histórico detalhado de ações e acessos para fins de auditoria.

3.5 Estabelecimento de uma Política de Governança

A UFVJM possui aprovada pela Comissão Interna de Implementação da LGPD a Política de Privacidade e Proteção de Dados Pessoais. Também foi apreciada e aprovada pelo Comitê de Governança, Riscos e Controle (CGIRC) a Política de Segurança da Informação (PSI). Desse modo, a UFVJM possui uma política de governança mínima capaz de garantir que os serviços de computação em nuvem resguardem os direitos dos proprietários de dados da comunidade acadêmica, considerando a migração para uma estrutura de nuvem pública. Podem-se destacar os seguintes pontos baseados nas Políticas de Privacidade e de Segurança da Informação da instituição:

3.5.1 Política de Segurança da Informação (PSI): A PSI da UFVJM define diretrizes para assegurar a autenticidade, confidencialidade, disponibilidade e integridade das informações produzidas ou custodiadas pela universidade. Essas diretrizes determinam que os dados estarão protegidos por medidas apropriadas contra ameaças e acessos não autorizados, o que é essencial ao adotar serviços de nuvem pública.

3.5.2 Controle de Acesso e Classificação de Dados: a PSI impõe práticas de controle de acesso (por exemplo, autenticação e restrição de acesso) e classifica as informações em diferentes níveis de confidencialidade (públicas, restritas, secretas e pessoais). Isso assegura que a UFVJM tem critérios estabelecidos para regular o acesso de acordo com a sensibilidade dos dados, garantindo a proteção necessária durante e após a migração para a nuvem.

3.5.3 Política de Privacidade e Proteção de Dados Pessoais: alinhada à LGPD, essa política enfatiza o respeito à privacidade e a coleta mínima de dados pessoais necessários para atividades institucionais. A governança em proteção de dados considera, ainda, medidas técnicas e administrativas para mitigar riscos, o que é crucial em um ambiente de nuvem onde dados de toda a comunidade acadêmica estarão armazenados.

3.5.4 Gerenciamento de Riscos e Continuidade de Negócios: a PSI contempla um processo de gerenciamento de riscos e indica os parâmetros nos quais a elaboração um plano de continuidade de negócios deve se basear, buscando assegurar a recuperação rápida e segura dos dados e serviços da UFVJM após eventos adversos. Isso é especialmente relevante ao migrar sistemas *on-premises* (data center local) para a nuvem, pois assegura que a instituição pode responder a incidentes com o apoio do provedor de nuvem.

3.5.5 Conformidade com Normas e Requisitos Legais: ambas as políticas mencionam a conformidade com legislações, como a Lei de Acesso à Informação e a LGPD, e com padrões de segurança (como ISO/IEC 27001). A UFVJM assegura que as práticas de proteção de dados estão em conformidade com normas de segurança internacionalmente reconhecidas, as quais também são adotadas pelos principais provedores de nuvem.

Essas políticas constituem um arcabouço de governança que, ao ser aplicado aos serviços de nuvem, garante a proteção dos dados da comunidade acadêmica em todas as etapas, desde o controle de acesso até a preservação e recuperação dos dados. Isso é essencial para a transição segura para uma infraestrutura de nuvem pública.

3.6 Diretrizes de Uso Seguro de Software e de Serviços de Computação em Nuvem:

Mediante análise dos sistemas da UFVJM, não foi identificado impedimento, do ponto de vista de segurança e conformidade legal, para a migração de nenhum deles para a nuvem.

Essa justificativa baseia-se em dois fatores principais:

3.6.1 Natureza dos Dados e Classificação de Segurança: a UFVJM não lida com dados classificados como "ultrassecretos" ou "secretos" conforme a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Instrução Normativa GSI/PR nº 5/2021. Os dados armazenados e tratados nos sistemas da UFVJM são predominantemente de natureza administrativa e acadêmica, sem incluir informações de alta sensibilidade ou que comprometam a segurança nacional.

3.6.2 Impacto Operacional e Continuidade dos Serviços Públicos: a UFVJM não possui sistemas críticos para a continuidade de serviços essenciais ao funcionamento do Estado, segundo os critérios estabelecidos pela Portaria SGD/MGI nº 5.950/2023. Embora os dados

da universidade sejam importantes para a sua operação, a sua indisponibilidade temporária não traria impactos críticos à continuidade dos serviços públicos essenciais em âmbito nacional.

Considerando esses fatores, pode-se concluir que os sistemas da UFVJM são elegíveis para migração para a nuvem pública ou híbrida, pois atendem aos requisitos de segurança para tal ambiente. Mesmo assim, é recomendável a aplicação de políticas de segurança adicionais, como criptografia e controles de acesso robustos, garantindo que a proteção dos dados acadêmicos e administrativos da universidade esteja em conformidade com a LGPD e as diretrizes de segurança vigentes.

3.7 Avaliação das condições de infraestrutura de TIC da UFVJM para utilizar serviços de computação em nuvem

A UFVJM possui condições mínimas de infraestrutura de TIC para operar com sistemas hospedados em ambiente de nuvem, substituindo o atual data center local, principalmente pelas seguintes razões:

3.7.1 Largura de Banda e Conectividade: O campus JK da UFVJM, onde está localizado o data center principal, é atendido por um contrato de fornecimento de link de internet com a Rede Nacional de Pesquisa (RNP). Este link tem se mostrado suficiente para atender a demanda de conectividade, suportando as atividades acadêmicas, administrativas e de acesso aos sistemas pela comunidade acadêmica.

3.7.2 Escalabilidade da Infraestrutura de Conectividade: Caso a migração dos sistemas para a nuvem resulte em aumento significativo no tráfego de dados, a UFVJM tem a possibilidade de iniciar tratativas com a RNP para ampliar a largura de banda do link atual. Alternativamente, há a opção de contratar um link de internet adicional com outro provedor, garantindo assim a flexibilidade necessária para ajustar a capacidade da rede conforme as novas necessidades de uso de computação em nuvem.

Essa infraestrutura de conectividade assegura que a UFVJM está preparada para adotar serviços de nuvem, proporcionando desempenho adequado e resiliência no acesso aos

sistemas em nuvem, sem comprometer a experiência e as atividades da comunidade acadêmica.

3.8 Diretrizes Básicas de Governança para o Uso de Computação em Nuvem

3.8.1 Alinhamento Estratégico e Gestão de Governança

- Objetivo: garantir que o uso da nuvem esteja em conformidade com as estratégias e metas institucionais da UFVJM, promovendo eficiência e inovação.
- Responsável: CGIRC (Comitê de Gestor de TIC da UFVJM)
- Ações:
  - Definir e revisar políticas para o uso de serviços em nuvem, assegurando que estejam alinhadas com as diretrizes do Governo Federal e as necessidades da UFVJM.
  - Aprovar a estratégia de uso de software e computação em nuvem, levando em consideração segurança, custo, e requisitos das áreas de negócio.
  - Monitorar a execução da governança em nuvem através de relatórios de desempenho e indicadores de conformidade fornecidos pelas áreas operacionais e financeiras.

3.8.2 Gestão Operacional dos Serviços de Nuvem

- Objetivo: assegurar a implementação, monitoramento e manutenção dos serviços de nuvem, promovendo a continuidade de serviços e o atendimento aos requisitos técnicos e de segurança.
- Responsável: Área de TI (servidores da STI) supervisionada pelo Superintendente de Tecnologia da Informação
- Ações:
  - Gerenciar o provisionamento de recursos e monitorar o desempenho dos serviços em nuvem, mantendo a disponibilidade e a segurança dos sistemas.

        - Prestar suporte técnico às áreas demandantes dos sistemas, atendendo a incidentes e promovendo a integração dos serviços com a infraestrutura existente.
        - Colaborar com a empresa contratada (provedor ou agente integrador) para alinhar o atendimento técnico aos padrões de qualidade e eficiência exigidos pela UFVJM.
        - Identificar, em colaboração com os demais agentes envolvidos, oportunidades de economia e otimização de recursos, assegurando o cumprimento dos limites orçamentários.

3.8.3 Segurança da Informação e Gestão de Incidentes

- Objetivo: proteger os dados institucionais e garantir a conformidade com as normas de segurança, monitorando incidentes e aplicando as melhores práticas de segurança.
- Responsável: Gestor de Segurança da Informação e ETIR (Equipe de Prevenção, Tratamento e Resposta a Incidentes)
- Ações:
    - Implementar controles de segurança específicos para o ambiente de nuvem, como autenticação multifatorial, criptografia de dados e monitoramento contínuo de acessos.
    - Analisar e responder a incidentes de segurança, colaborando com a empresa fornecedora dos serviços para corrigir vulnerabilidades.
    - Atualizar políticas e treinamentos de segurança de acordo com as práticas de segurança recomendadas pelo Governo Federal (notadamente o CTIR), orientando as áreas demandantes sobre práticas seguras.

3.8.4 Planejamento Orçamentário e Controle de Custos

- Objetivo: assegurar a gestão eficiente dos custos de serviços em nuvem, alinhando o orçamento com as prioridades institucionais.

- Responsável: Pró-Reitoria de Planejamento e Orçamento, em colaboração com a STI
- Ações:
  - Monitorar o consumo e os custos dos serviços de nuvem, revisando periodicamente o orçamento e solicitando ajustes para um uso eficiente.
  - Estar em contato permanente com a área operacional para ajustar o modelo de contratação às necessidades de expansão ou redução de recursos, conforme o interesse e necessidade institucional.

3.8.5 Gestão de Demandas e Relacionamento com as Áreas de Negócio

- Objetivo: Identificação e priorização de demandas, assegurando que o uso da nuvem seja compatível com suas atividades e processos.
- Responsável: Representantes das áreas de negócio (Pró-Reitores e Diretores de Unidades Acadêmicas), com apoio da STI
- Ações:
  - Levantar e priorizar as necessidades das áreas demandantes, assegurando que os serviços contratados suportem os processos acadêmicos e administrativos.
  - Colaborar com a STI para definir requisitos técnicos e validar soluções que atendam às demandas específicas de cada área.

3.8.6 Parceria e Alinhamento com a Empresa Contratada para Serviços de Nuvem

- Objetivo: Garantir que a empresa contratada opere de acordo com os padrões de segurança e qualidade necessários à UFVJM, promovendo uma colaboração alinhada com os interesses institucionais.
- Responsável: Área de TI (STI) e Superintendente de Tecnologia da Informação
- **Ações**:

- Estabelecer comunicação regular com a empresa para monitorar a qualidade dos serviços, alinhando expectativas e padrões operacionais.
- Definir processos de escalonamento para suporte técnico e resolução de incidentes, garantindo respostas rápidas e eficazes.
- Assegurar que a empresa cumpra com as políticas de segurança e privacidade, realizando auditorias e verificações de conformidade periodicamente.

3.8.6 Papéis e Responsabilidades dos Atores Organizacionais

3.8.6.1 CGIRC (Comitê Gestor de TIC): define as diretrizes estratégicas e assegura o alinhamento do uso da nuvem aos objetivos institucionais e às normas governamentais.

3.8.6.2 Superintendente de Tecnologia da Informação: supervisiona a STI e a implementação das soluções de nuvem, garantindo a continuidade e segurança dos serviços.

3.8.6.3 Área de TIC (STI): responsável pela gestão operacional dos serviços de nuvem, incluindo monitoramento, suporte técnico, e colaboração com o fornecedor para atendimento das demandas institucionais.

3.8.6.4 Gestor de Segurança da Informação e ETIR: implementam as políticas de segurança, realizam monitoramento contínuo e coordenam a resposta a incidentes de segurança.

3.8.6.5 Pró-Reitoria de Planejamento e Orçamento: coordena o planejamento e monitoramento de custos das contratações de serviços de nuvem efetivadas, alinhando o uso financeiro com as necessidades institucionais.

3.8.6.6 Representantes das Áreas de Negócio (Pró-Reitores e Diretores de Unidades Acadêmicas): trabalham com a STI para identificar demandas específicas, promovendo o uso dos recursos de nuvem de forma alinhada aos processos acadêmicos e administrativos.

3.8.6.7 Colaboradores da Empresa Contratada para prestação de Serviços de Nuvem: operam conforme as diretrizes da UFVJM, garantindo a continuidade e a segurança dos serviços, com suporte aos requisitos institucionais e resposta a incidentes.

Essas diretrizes de governança asseguram que o uso dos serviços de computação em nuvem pela UFVJM seja seguro, eficiente e alinhado aos objetivos estratégicos, promovendo uma abordagem colaborativa entre os setores da universidade e a empresa contratada.

3.9) Princípios Norteadores da Presente Estratégia

Os princípios norteadores dessa Estratégia de uso de software e serviços de computação em nuvem são os seguintes:

3.9.1. Cloud First: Esse princípio significa dar preferência à nuvem para novas aquisições de infraestrutura e software, determinando a escolha da nuvem sempre que essa opção for tecnicamente viável, financeiramente vantajosa e atender aos requisitos de segurança.

- Objetivo: Acelerar a inovação, reduzir custos com infraestrutura física, e aumentar a flexibilidade e escalabilidade.
- Benefícios: Redução de tempo para implantações, maior agilidade em operações e modernização tecnológica.

3.9.2. Refatoração, sempre que possível: Ao invés vez de mover a aplicação para a nuvem com o mínimo de mudanças em relação ao modo como ela se encontra hospedada localmente (como ocorre no princípio "*Lift and Shift*"), a Refatoração envolve a revisão e modificação do código e da arquitetura da aplicação para que ela aproveite de maneira mais eficiente as capacidades da nuvem.

Características da Refatoração:

- Maior eficiência e flexibilidade com recursos de nuvem.
- Melhor uso das tecnologias nativas da nuvem.

- Escalabilidade e desempenho aprimorados.
- Redução de custos de longo prazo pela otimização.
- Maior complexidade e tempo de migração:

3.9.3. Uso de *Broker Multicloud*: é uma camada de serviço que permite a gestão centralizada e a integração de múltiplas nuvens (públicas e/ou privadas). Essa prática facilita o uso simultâneo de diferentes provedores de nuvem, melhorando a flexibilidade e evitando a dependência de um único fornecedor.

- Objetivo: Permitir uma abordagem de nuvem híbrida ou *multicloud* que combine os melhores serviços de diferentes provedores, otimizando custos e recursos.
- Benefícios: Melhoria da redundância e resiliência dos sistemas, otimização de custos entre provedores e redução do risco de dependência exclusiva de um único fornecedor ou mesmo de um único provedor.

3.9.4. Elasticidade e Escalabilidade: utilizar a capacidade de ajuste dinâmico de recursos oferecida pela nuvem, tanto para aumentar (escalar) como para diminuir (reduzir) recursos com base na demanda. Essa elasticidade permite que as aplicações se adaptem automaticamente a flutuações de carga que existirem, de acordo com as demandas acadêmicas e administrativas ao longo do dia e da semana.

- Objetivo: Evitar sobrecarga de sistemas e otimizar o uso de recursos, garantindo que a infraestrutura se ajuste às necessidades reais.
- Benefícios: Redução de custos operacionais e melhoria da eficiência com uso racional de recursos.

3.9.5. Automação e Infraestrutura como Código (IaC): referem-se ao uso de scripts e ferramentas para gerenciar e provisionar recursos de nuvem de forma automática. Infraestrutura como Código permite que a configuração e o provisionamento sejam descritos em arquivos de código e aplicados automaticamente.

- Objetivo: Reduzir erros manuais, melhorar a padronização de ambientes e aumentar a agilidade de implantação.

- Benefícios: Melhoria da consistência e velocidade de *deploys*, facilidade de replicação de ambientes e redução de erros.

3.9.6. Responsabilidade Compartilhada: em ambientes de nuvem, a segurança e conformidade são de responsabilidade tanto do provedor de nuvem quanto dos clientes. O provedor garante a segurança da infraestrutura, enquanto o cliente é responsável pela segurança dos dados e das configurações.

- Objetivo: Garantir que as práticas de segurança estejam corretamente atribuídas entre cliente e provedor.
- Benefícios: Melhoria na segurança geral e clareza nas responsabilidades, reduzindo riscos de falhas por falta de proteção adequada.

3.10 Alinhamento com outros planos estratégicos da UFVJM

Em relação ao alinhamento dessa Estratégia com outros planos estratégicos da UFVJM, tem-se a seguinte situação:

3.10.1 O PDTI atual (2024-2028) está em fase final do processo de elaboração.

3.10.2 No PDI 2024-2028 da UFVJM, a Tecnologia da Informação é uma das áreas de apoio de Governança e Gestão para o cumprimento de sua missão.

3.10.3 Objetivo Estratégico OE.4 da Estratégia de Governança Digital 2020-2022: "*Ampliar o uso de novas tecnologias de informação e comunicação na educação.*"

3.10.4 Objetivo Estratégico 17 do Planejamento Estratégico Institucional (PEI) UFVJM 2021-2025: "*Aperfeiçoar os sistemas de informação e infraestrutura de tecnologia da informação (TI) da instituição em apoio ao ensino, pesquisa, pós-graduação, extensão e administração.*"

3.10.5 Plano de Contratações Anual (PCA), em seu Documento de Formalização da Demanda número 220/2023, tem como descrição do objeto: "*Plataforma de hospedagem de serviços em nuvem*".

3.11) Metas de benefícios e resultados esperados

Com a implantação da Estratégia de Uso de Software e Serviços em Nuvem na UFVJM, busca-se atingir os seguintes resultados, quantificados a partir de suas respectivas metas:

3.11.1. Redução de Custo Operacional e Financeiro para Manutenção de Data Center: Diminuir significativamente os custos relacionados à operação e manutenção dos data centers locais no Campus JK, tais como despesas com serviços de manutenção em hardware, sistema de refrigeração, energia ininterrupta, energia secundária, atualização de software, aquisição de hardware e outros custos de infraestrutura física.

- Meta: Obter uma economia anual de pelo menos 50% nos custos relacionados ao data center, em 2 anos, contados a partir do início da migração das cargas de trabalho para a nuvem. Isso permitirá o redirecionamento de recursos para outras áreas de TIC e para projetos estratégicos institucionais.

3.11.2. Escalabilidade de Recursos e Capacidade de Ajuste Sob Demanda: Assegurar que os recursos de processamento, armazenamento e rede possam ser dimensionados conforme as necessidades da UFVJM, atendendo picos de demanda sem necessidade de grandes investimentos em infraestrutura.

- Meta: Atingir a capacidade de expansão de até 100% dos recursos computacionais durante períodos de alta demanda dos sistemas e uma redução proporcional nos períodos de baixa, ajustando os custos ao uso real dos recursos e garantindo eficiência no consumo.

3.11.3. Aumento da Disponibilidade dos Sistemas e Serviços, com Foco em Acessibilidade Fora do Campus JK**:** Proporcionar uma disponibilidade contínua de sistemas e serviços críticos para que estejam acessíveis a toda a comunidade acadêmica, especialmente a partir de locais externos ao campus JK.

- Meta: Alcançar uma disponibilidade de 99,5% para sistemas e serviços em nuvem, com tempos de inatividade mínimos, apoiando o trabalho remoto e acesso remoto dos estudantes, servidores, demais colaboradores e comunidade externa.

3.11.4. Capacidade para Atendimento de Novos Sistemas, Serviços e Atualizações Tecnológicas: Ampliar a capacidade de infraestrutura para suportar novos sistemas acadêmicos, administrativos e outros serviços, assim como facilitar o processo de atualizações e melhorias contínuas de sistemas já em operação.

- Meta: Implementar uma infraestrutura que permita o acréscimo de, ao menos, 3 novos sistemas por ano, sem comprometer o desempenho daqueles já existentes, com capacidade de atualização contínua de software e rápida adaptação às novas demandas tecnológicas.

3.11.5. Fortalecimento da Segurança e das Práticas de Governança de TI: Melhorar a segurança dos dados e dos sistemas da UFVJM, implementando práticas avançadas de proteção em ambiente de nuvem, como criptografia, controles de acesso rigorosos, e monitoramento contínuo de vulnerabilidades.

- Meta: Reduzir pela metade o número de incidentes relacionados à segurança da informação comparado ao ambiente local, promovendo a integridade e a proteção dos dados institucionais e alinhando-se aos padrões e diretrizes de governança e segurança exigidos pela legislação.

3.11.6. Capacidade de Adoção e Integração de Tecnologias Emergentes: Facilitar a adoção de novas tecnologias em nuvem, como inteligência artificial, *big data* e ferramentas de análise avançada, promovendo inovação e suporte a projetos de pesquisa e extensão.

- Meta: Garantir que os sistemas de computação em nuvem estejam preparados para a integração com tecnologias emergentes, permitindo à UFVJM adotar inovações rapidamente e de forma eficiente.

3.12 Considerações sobre capacitação da equipe da UFVJM

A equipe da Superintendência de Tecnologia da Informação (STI) da UFVJM precisa desenvolver habilidades e conhecimentos em áreas críticas para operar e gerenciar os recursos em nuvem. Abaixo estão os principais requisitos de treinamento e capacitação elencados:

Principais Capacidades e Habilidades Necessárias:

3.12.1 Administração e Operação de Infraestruturas em Nuvem:

- Capacitação na utilização de recursos de IaaS (Infraestrutura como Serviço), PaaS (Plataforma como Serviço) e SaaS (Software como Serviço).
- Compreensão dos processos de provisionamento, configuração e otimização de recursos, com foco na eficiência operacional e redução de custos.

3.12.2 Gestão de Segurança em Nuvem:

- Treinamento em políticas de segurança e práticas de governança específicas para ambientes em nuvem, como criptografia de dados, controle de acesso, monitoramento de ameaças e resposta a incidentes.
- Habilidades em configurações de segurança e uso de ferramentas de IAM (Gerenciamento de Identidade e Acesso) para gerenciar permissões e autenticação multifatorial.

3.12.3 Automação e Gerenciamento de Recursos:

- Domínio de ferramentas de automação, como Infraestrutura como Código (IaC), para provisionamento e orquestração automática de recursos.
- Capacitação no uso de scripts e automação para gerenciamento e otimização dos recursos em nuvem, minimizando a necessidade de intervenções manuais e maximizando a eficiência.

3.12.4 Monitoramento e Análise de Desempenho:

- Treinamento em ferramentas de monitoramento contínuo para avaliar o desempenho dos serviços em nuvem e identificar possíveis gargalos ou áreas de melhoria.
- Habilidades em configurar alertas e relatórios de desempenho, garantindo que o ambiente em nuvem atenda às necessidades de disponibilidade e desempenho esperadas pela UFVJM.

3.12.5 Gerenciamento de Custos e Orçamento em Nuvem:

- Capacitação para monitoramento de custos e uso eficiente dos recursos, com habilidades para identificar e ajustar recursos para reduzir gastos.
- Capacidade para implementar políticas de controle financeiro e utilizar ferramentas de previsão de custos para assegurar o alinhamento com o orçamento institucional.

3.12.6 Migração e Integração de Sistemas:

- Treinamento para realizar migrações de sistemas do data center local para a nuvem, incluindo planejamento, execução e validação das migrações.
- Habilidades para integrar serviços e dados entre a infraestrutura local e a nuvem, assegurando a interoperabilidade e a continuidade dos serviços.

3.13 Considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços

Para garantir a portabilidade e interoperabilidade dos sistemas da UFVJM e mitigar o risco de dependência tecnológica ou "aprisionamento ao provedor" ao migrar para a nuvem, é fundamental adotar medidas que permitam flexibilidade e compatibilidade entre diferentes plataformas de nuvem. A seguir, são listadas as principais medidas para atender a esses objetivos:

3.13.1. Adoção de um Agente Integrador (Cloud Broker) Multi-nuvem: a utilização de um agente integrador multi-nuvem permite gerenciar e integrar recursos de diferentes

provedores de nuvem, facilitando a movimentação de cargas de trabalho entre ambientes de nuvem distintos.

- Benefício esperado: desde o início da jornada para a nuvem, a UFVJM poderá migrar e adaptar suas operações em diferentes ambientes de nuvem, promovendo flexibilidade e minimizando a dependência de um único provedor.

3.13.2. Implementação de Arquitetura Baseada em Contêineres: os contêineres, como Docker e Kubernetes, isolam aplicações do ambiente subjacente, permitindo que elas funcionem de maneira consistente em qualquer infraestrutura compatível com contêineres.

- Benefício esperado: facilita a portabilidade e a interoperabilidade entre diferentes provedores de nuvem, permitindo que os sistemas sejam migrados sem modificações significativas.

3.13.3. Armazenamento de Dados em Formatos Padrão e Abertos: utilizar formatos de dados amplamente aceitos (como JSON, XML, CSV) facilita a migração e integração de dados entre sistemas de diferentes provedores.

- Benefício esperado: Permite a exportação e transferência de dados entre ambientes de nuvem com mínima necessidade de conversão, melhorando a portabilidade dos dados.

3.13.4. Adoção de Infraestrutura como Código (IaC) Multi-nuvem: tais ferramentas, como Terraform e Ansible, permitem gerenciar a infraestrutura de forma padronizada e automatizada, independentemente do provedor de nuvem.

- Benefício esperado: Facilita a reprodução e migração da infraestrutura para outras plataformas, permitindo que as configurações sejam replicadas de forma consistente em múltiplos ambientes.

3.13.5. Divisão dos Sistemas em Arquitetura de Microsserviços: A segmentação de sistemas em microsserviços desacoplados facilita a movimentação de partes específicas do sistema entre diferentes ambientes, sem a necessidade de migrar o sistema completo.

- Benefício: aumenta a flexibilidade para mover partes do sistema, facilitando a integração com outros serviços e minimizando o aprisionamento tecnológico.

3.13.6. Estabelecimento de Contratos com Acordos de Serviço Flexíveis e Cláusulas de Portabilidade: é importante haver a previsão nos Termos de Referência de que os contratos com os provedores de nuvem incluam acordos de serviço específicos para portabilidade e cláusulas que garantam apoio na transição para outros ambientes de cloud.

- Benefício: Garante suporte técnico na migração para outros provedores e reduz custos e barreiras para a portabilidade.

3.13.7. Implementação de Backup e Replicação de Dados em Ambientes Multi-nuvem: ter backups e replicações de dados em diferentes provedores de nuvem aumenta a segurança dos dados e facilita a recuperação em caso de necessidade de mudança de provedor.

- Benefício: permite que a UFVJM mova dados para um novo ambiente de forma rápida e segura, mitigando a dependência de um único provedor.

3.13.8. Capacitação da Equipe em Estratégias Multi-nuvem e Interoperabilidade: Treinar a equipe da STI em práticas de multi-nuvem e interoperabilidade, de modo a permitir a gestão independente e competente de diferentes plataformas.

- Benefício: a equipe estará preparada para operar e migrar serviços entre diferentes nuvens, promovendo um ambiente flexível e independente.

3.14 Requisitos Regulatórios e de Conformidade

Para a contratação e utilização de recursos de computação em nuvem, a UFVJM, como autarquia federal da área de educação, precisa seguir uma série de requisitos regulatórios e de conformidade que garantem a segurança, privacidade e conformidade legal dos dados e sistemas institucionais. Abaixo estão listados os principais requisitos regulatórios e normas aplicáveis, com sua respectiva descrição e escopo de aplicação na UFVJM:

3.14.1. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018

- Descrição: estabelece diretrizes para o tratamento de dados pessoais no Brasil, exigindo proteção à privacidade, transparência sobre a utilização e compartilhamento de informações pessoais, e direitos dos titulares.
- Aplicação: a UFVJM deve assegurar que os dados pessoais processados na nuvem estejam protegidos conforme os princípios de segurança, com práticas de privacidade que incluem controle de acesso e consentimento.

3.14.2. Instrução Normativa GSI/PR nº 5/2021

- Descrição: estabelece requisitos de segurança da informação para órgãos e entidades da Administração Pública Federal, com foco na confidencialidade, integridade, disponibilidade e autenticidade da informação.
- Aplicação: a UFVJM deve garantir que os serviços em nuvem atendam a esses requisitos de segurança, adotando políticas e práticas de proteção para mitigar ameaças e vulnerabilidades.

3.14.3. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022

- Descrição: define as regras para a contratação e uso de soluções de tecnologia da informação e comunicação (TIC) no âmbito da administração pública federal, abordando temas como planejamento, avaliação de riscos e governança.
- Aplicação: a UFVJM deve assegurar que suas contratações de serviços em nuvem estejam em conformidade com os processos de governança e requisitos de segurança definidos pela IN nº 94.

3.14.4. Portaria MEC nº 315/2018 - Acervo Acadêmico Digital

- Descrição: estabelece normas e orientações sobre a preservação e armazenamento digital de acervos acadêmicos, incluindo dados acadêmicos, registros de alunos e documentos institucionais.

- Aplicação: a UFVJM deve assegurar que os registros acadêmicos digitalizados em nuvem sejam armazenados com integridade, autenticidade e segurança, conforme exigências específicas para acervos acadêmicos.

3.14.5. ISO/IEC 27001 - Sistema de Gestão de Segurança da Informação

- Descrição: norma internacional que especifica os requisitos para implementação de um sistema de gestão de segurança da informação, com ênfase em avaliação de riscos e proteção de dados.
- Aplicação: a UFVJM deve priorizar provedores de nuvem certificados pela ISO/IEC 27001, garantindo que a segurança da informação esteja alinhada a padrões reconhecidos mundialmente.

3.14.6. ISO/IEC 27017 - Controles de Segurança em Serviços de Computação em Nuvem

- Descrição: complementa a ISO 27001 com controles de segurança específicos para serviços em nuvem, abordando a responsabilidade compartilhada entre provedores e clientes.
- Aplicação: a UFVJM deve considerar a conformidade com a ISO 27017 para garantir práticas robustas de segurança na nuvem e uma clara divisão de responsabilidades.

3.14.7. ISO/IEC 27018 - Proteção de Dados Pessoais em Ambientes de Nuvem Pública

- Descrição: norma que define controles para a proteção de dados pessoais em ambientes de nuvem pública, assegurando práticas que preservem a privacidade dos dados.
- Aplicação: a UFVJM deve preferir provedores que sigam a ISO 27018, especialmente ao lidar com dados pessoais, para garantir o alinhamento com a LGPD e proteção avançada contra acessos não autorizados.

3.14.8. Marco Civil da Internet - Lei nº 12.965/2014

- Descrição: estabelece direitos e deveres para o uso da internet no Brasil, assegurando proteção de dados pessoais, privacidade dos usuários e integridade da informação.

- Aplicação: a UFVJM deve garantir que o armazenamento e o tratamento de dados na nuvem respeitem os princípios de privacidade e segurança conforme os direitos estabelecidos no Marco Civil.

3.14.9. Política Nacional de Segurança da Informação (PNSI) - Decreto nº 9.637/2018

- Descrição: define princípios e diretrizes para a segurança da informação na Administração Pública Federal.
- Aplicação: a UFVJM deve assegurar que seus sistemas e dados estejam protegidos segundo a PNSI, promovendo segurança nos dados estratégicos e proteção contra ameaças.

3.14.10. Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011

- Descrição: regula o acesso público a informações e documentos do governo, exigindo transparência e acesso à informação, com proteção de dados sensíveis e sigilosos.
- Aplicação: a UFVJM deve garantir que os dados públicos estejam acessíveis e protegidos conforme a LAI, respeitando a privacidade de dados restritos e sigilosos.

3.14.11. Resolução CGE nº 65/2020 - Arquivamento e Preservação Digital

- Descrição: estabelece diretrizes para a preservação de documentos digitais na Administração Pública, garantindo integridade, autenticidade e acesso contínuo.
- Aplicação: a UFVJM deve assegurar que documentos arquivados na nuvem cumpram os requisitos de preservação digital, com armazenamento seguro e acessível de longo prazo.

3.14.12. Portaria SGD/MGI nº 5.950/2023 - Modelo de Contratação de Software e Serviços de Computação em Nuvem

- Descrição: define diretrizes e requisitos para contratação e uso de serviços de computação em nuvem na Administração Pública Federal, com foco em segurança, governança e conformidade.

- Aplicação: a UFVJM deve seguir as orientações desta portaria para realizar contratações em nuvem que estejam alinhadas a boas práticas de segurança e gerenciamento.

3.15 Indicação da Estratégia de Saída da Nuvem

A Estratégia de Saída da Nuvem visa garantir que a universidade possa migrar com segurança e eficiência seus sistemas e dados para outra solução, seja de volta para a infraestrutura local ou para outro provedor de nuvem, caso necessário. Esta estratégia considera aspectos de dependência, portabilidade e conformidade com as diretrizes da Instrução Normativa GSI/PR nº 5/2021 e da Portaria SGD/MGI nº 5.950/2023. A seguir se encontram as principais ações a serem consideradas para efetivação dessa estratégia.

3.15.1. Análise de Dependências e Planejamento de Portabilidade

- Objetivo: Realizar um mapeamento detalhado das dependências existentes dos sistemas em nuvem para garantir que a migração para um novo ambiente (local ou outro provedor) ocorra sem perda de dados ou funcionalidades.
- Ações:
    - Mapear os serviços, aplicativos e dados críticos que precisam ser migrados.
    - Adotar formatos de dados e APIs abertas, sempre que possível, para minimizar problemas de compatibilidade e assegurar a portabilidade.
    - Documentar os requisitos de interoperabilidade dos sistemas, incluindo especificações técnicas e configurações.

3.15.2. Plano de Backup e Redundância de Dados

- Objetivo: Assegurar que os dados armazenados em nuvem tenham cópias redundantes, protegidas e acessíveis em caso de migração.
- Ações:
    - Implementar políticas de backup regulares, com cópias armazenadas em local seguro fora da infraestrutura principal do provedor de nuvem.

- Manter uma redundância de dados para suportar a continuidade de operações durante o processo de migração, evitando a perda de informações e garantindo o acesso aos sistemas críticos.

3.15.3. Contratos de Apoio mediante Sistema de Registro de Preços (SRP)

- Objetivo: Preparar uma estrutura contratual que permita flexibilidade e suporte durante o processo de saída, inclusive prevendo a contratação de infraestrutura local.
- Ações:
  - Especificar uma contratação que permita o apoio do provedor de nuvem durante a fase de transição para fora da nuvem, incluindo o suporte técnico necessário para a migração dos dados.
  - Considerar o uso de contratações por Sistema de Registro de Preços (SRP) para adquirir e implantar uma infraestrutura de data center local, caso seja necessário retornar as operações para a infraestrutura interna da UFVJM.

3.15.4. Preparação de Infraestrutura Local para Continuidade

- Objetivo: Garantir que, em caso de retorno à infraestrutura local, a UFVJM possua um ambiente seguro e tecnologicamente atualizado para suportar a carga de trabalho.
- Ações:
  - Planejar a aquisição de uma infraestrutura hiperconvergente para data center, que inclui soluções de virtualização, conteinerização e apoio a aplicações críticas.
  - Incorporar estruturas de apoio ao data center local, como sistemas de energia ininterrupta (nobreaks), energia secundária (geradores), refrigeração adequada e sistemas de combate e prevenção a incêndios.
  - Garantir que as soluções contratadas para o data center estejam alinhadas com as práticas de modernização e segurança estabelecidas pela Portaria SGD/MGI nº 5.950/2023.

3.15.5. Execução de Testes de Migração e Portabilidade

- Objetivo: Testar a viabilidade de portabilidade para a infraestrutura local ou outro ambiente de nuvem com antecedência, mitigando riscos no processo de saída.
- Ações:
    - Realizar simulações de migração e testes de portabilidade com amostras de dados e sistemas para avaliar compatibilidades e potenciais problemas.
    - Ajustar os sistemas e fluxos de trabalho com base nos resultados dos testes para assegurar uma migração mais fluida e segura.

3.15.6. Documentação e Registro de Atividades

- Objetivo: Manter registros detalhados de todas as atividades, configurações e processos durante o uso de nuvem e a migração de saída.
- Ações:
    - Documentar os passos técnicos da migração, configurações de sistemas, processos de backup e instruções de configuração para o ambiente de destino.
    - Manter registros dos contratos, das políticas de backup e de recuperação de dados, de modo a garantir que todas as etapas da saída sejam bem documentadas e auditáveis.

3.15.7. Suporte Continuado Pós-Migração

- Objetivo: Estabelecer a contratação de um plano de suporte para garantir a continuidade das operações e o rápido atendimento de possíveis problemas após a migração.
- Ações:
    - Prever em contrato um possível aditamento para um período de suporte técnico adicional com o provedor de nuvem atual, se aplicável, para a resolução de possíveis problemas após a migração.
    - Compor uma equipe de resposta interna ou contratar suporte externo especializado para auxiliar no ajuste do ambiente pós-migração e responder a eventuais falhas ou desafios técnicos.

3.16 Análise de Riscos

A seguir se encontra a análise de riscos realizada para o processo de migração dos sistemas da UFVJM da infraestrutura de data center local para a nuvem.

3.16.1. Risco de Perda de Dados Durante a Migração

- Descrição: Existe o risco de perda ou corrupção de dados durante o processo de migração devido a falhas técnicas, erros de configuração ou falhas na transferência.
- Impacto: Alto, pois a perda de dados pode comprometer a integridade de informações críticas para as operações acadêmicas e administrativas.
- Medidas de Mitigação:
    - Implementar um plano de backup completo dos dados antes da migração, com múltiplas cópias em local seguro.
    - Realizar testes de migração em pequena escala antes da migração integral.
    - Monitorar e validar a integridade dos dados após a transferência.

3.16.2. Dependência Excessiva do Provedor de Nuvem (“Vendor Lock-in”)

- Descrição: A UFVJM pode se tornar dependente de um único provedor de nuvem, dificultando futuras migrações ou a diversificação de serviços.
- Impacto: Médio, pois restringe a flexibilidade e pode acarretar em custos elevados para adaptação a um novo provedor.
- Medidas de Mitigação:
    - Adotar padrões abertos e compatíveis com múltiplos ambientes de nuvem (multi-cloud).
    - Implementar arquitetura baseada em contêineres e utilizar infraestrutura como código (IaC) para facilitar a portabilidade entre provedores.
    - Contratar um broker *multi-cloud* para gerenciar e diversificar o uso da nuvem desde o início da migração das cargas de trabalho.

3.16.3. Risco de Incompatibilidade com Aplicações Existentes

- Descrição: Algumas aplicações podem não ser compatíveis com a nova infraestrutura em nuvem, exigindo adaptações ou modificações no código.
- Impacto: Médio, pois pode atrasar a implementação e acarretar custos adicionais para adequação.
- Medidas de Mitigação:
    - Realizar uma análise de compatibilidade antes da migração.
    - Priorizar a refatoração das aplicações para que aproveitem as capacidades da nuvem.
    - Estabelecer um plano de adaptação e testes de compatibilidade para cada sistema.

3.16.4. Risco de Interrupção dos Serviços durante a Migração

- Descrição: Durante o processo de migração, os sistemas podem apresentar indisponibilidade temporária, impactando atividades acadêmicas e administrativas.
- Impacto: Alto, uma vez que a interrupção pode causar transtornos, especialmente em períodos críticos como matrículas ou processos seletivos.
- Medidas de Mitigação:
    - Planejar a migração em horários e períodos de menor atividade.
    - Configurar uma infraestrutura híbrida temporária para garantir que serviços críticos continuem operacionais durante a transição.
    - Notificar previamente os usuários e preparar equipe para suporte caso surja algum imprevisto.

3.16.5. Risco de Falhas de Segurança e Violação de Dados

- Descrição: Durante a migração e operação em nuvem, os dados podem estar vulneráveis a violações de segurança e acessos não autorizados.
- Impacto: Alto, porque pode haver comprometimento da segurança dos dados acadêmicos e administrativos.
- Medidas de Mitigação:
    - Implementar criptografia de dados em trânsito e em repouso.

    - Estabelecer controle de acesso rigoroso e autenticação multifator para todas as aplicações e dados.
    - Monitorar continuamente as atividades e implantar uma política de resposta rápida a incidentes de segurança.

3.16.6. Risco de Aumento de Custos Operacionais na Nuvem

- Descrição: O uso em excesso ou falta de monitoramento dos recursos em nuvem pode gerar aumento inesperado dos custos financeiros.
- Impacto: Médio a Alto, pois pode comprometer o orçamento destinado às operações de TI.
- Medidas de Mitigação:
    - Utilizar ferramentas de monitoramento para controle de consumo e custo, além de configurar alertas para picos de uso.
    - Realizar auditorias periódicas para identificar e ajustar recursos subutilizados ou superdimensionados.
    - Estabelecer um plano de gestão de custos com a Pró-Reitoria de Planejamento e Orçamento e Equipe de Fiscalização do Contrato.

3.16.7. Risco de Desempenho Insuficiente dos Sistemas

- Descrição: Algumas aplicações podem apresentar queda de desempenho devido à latência ou limitações da infraestrutura em nuvem.
- Impacto: Médio, na medida em que a lentidão no acesso pode prejudicar a experiência dos usuários e a eficiência das operações.
- Medidas de Mitigação:
    - Analisar previamente os requisitos de desempenho dos sistemas e selecionar a configuração adequada de nuvem para a arquitetura definida.
    - Utilizar balanceamento de carga e otimizar o uso de rede para minimizar a latência.
    - Configurar redundância geográfica para melhorar a disponibilidade.

3.16.8. Risco de Não Conformidade com Regulamentos e Normas

- Descrição: A UFVJM pode enfrentar dificuldades para garantir conformidade com regulamentações como a LGPD e a Instrução Normativa GSI/PR nº 5/2021 em ambiente de nuvem.
- Impacto: Alto, porque pode resultar em penalidades, sanções e prejuízos à reputação da instituição.
- Medidas de Mitigação:
    - Contratar provedores de nuvem que possuam certificações de conformidade (ISO 27001, ISO 27017, ISO 27018).
    - Implementar controles de segurança e proteção de dados, incluindo políticas de privacidade e gerenciamento de auditorias.
    - Realizar treinamentos contínuos da equipe para assegurar que os requisitos regulatórios e de conformidade sejam atendidos.

IV - DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

A UFVJM deve atender a uma série de requisitos para garantir a segurança da informação e a conformidade com as normas aplicáveis. Com base na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, são descritos abaixo os principais aspectos e medidas de segurança para o uso seguro de computação em nuvem.

4.1. Proteção da Confidencialidade dos Dados

- Criptografia de Dados: Implementar criptografia para dados em trânsito e em repouso, assegurando a confidencialidade das informações sensíveis e protegendo contra acessos não autorizados. A criptografia deve seguir os padrões recomendados pelo Governo Federal.
- Gestão de Identidades e Acessos (IAM): Estabelecer políticas de controle de acesso com autenticação multifatorial para garantir que somente usuários autorizados possam acessar os sistemas e dados críticos.

4.2. Garantia de Integridade das Informações

- Controle de Alterações e Registros de Log: Monitorar e registrar todas as atividades de acesso e modificações nos sistemas e dados. O armazenamento e análise de logs devem ser realizados para garantir a rastreabilidade das operações e facilitar auditorias de segurança.
- Auditoria Regular e Monitoramento Contínuo: Realizar auditorias periódicas e monitoramento contínuo dos sistemas e serviços em nuvem para detectar alterações ou anomalias que possam comprometer a integridade dos dados.

4.3. Disponibilidade e Continuidade de Serviços

- Planos de Recuperação e Redundância: Desenvolver e implementar planos de recuperação de desastres que incluam backup regular dos dados e recursos de redundância para minimizar interrupções nos serviços, além da execução periódica de testes de restauração.
- Monitoração de Desempenho e Capacidade: Realizar o monitoramento da capacidade e do desempenho dos serviços para garantir a continuidade das operações e prevenir quedas de disponibilidade.

4.4. Segurança contra Ameaças Cibernéticas

- Proteção contra Malware e Ataques: Implementar *firewalls*, sistemas de proteção contra *malware* e sistemas de detecção e prevenção de intrusões (IDS/IPS) para mitigar riscos de ataques externos e proteger o ambiente de nuvem.
- Plano de Resposta a Incidentes: Estabelecer um plano de resposta para incidentes de segurança, incluindo procedimentos para identificar, conter, erradicar e recuperar os sistemas afetados. Este plano deve ser revisado e atualizado regularmente.

4.5. Segurança Física e Ambiental

- Ambiente de Armazenamento de Dados Seguro: Assegurar que os provedores de nuvem adotem medidas de segurança física para proteger os data centers onde os

dados da UFVJM são armazenados, incluindo controle de acesso ao ambiente físico, monitoramento e prevenção contra incêndios e desastres naturais.

4.6. Conformidade e Governança

- Certificações e Conformidade com Normas: Escolher provedores de nuvem que possuam certificações reconhecidas, como ISO/IEC 27001 e ISO/IEC 27017, para garantir que seus processos de segurança estão alinhados às melhores práticas internacionais.
- Revisão e Auditoria de Conformidade: Realizar revisões periódicas e auditorias de conformidade para assegurar que o ambiente de nuvem está em consonância com as regulamentações, como a LGPD e as diretrizes da Instrução Normativa GSI/PR nº 5.

4.7. Gerenciamento de Riscos e Avaliação Contínua

- Análise e Gestão de Riscos: Realizar análises regulares de risco para identificar e mitigar vulnerabilidades associadas ao uso de computação em nuvem, com base na criticidade dos sistemas e dados tratados.
- Planejamento de Contingência: Desenvolver planos de contingência para eventuais falhas de segurança ou indisponibilidade, assegurando a capacidade de resposta rápida e mitigação dos impactos operacionais.

ASSINATURAS

<O documento deve ser assinado por membros do Comitê de Governança Digital ou instância equivalente ou superior do órgão ou entidade.>