ANEXO - ESTRATÉGIA DE USO DE SERVIÇOS E COMPUTAÇÃO EM NUVEM

1. Objetivo

Este documento dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito da instituição. O escopo abrange as novas contratações de software e de serviços de computação em nuvem aderentes.

Os principais objetivos e necessidades de negócio a serem alcançados são:

- Maior controle e administração dos custos com armazenamento e processamento de dados;
- Agilidade e escalabilidade para armazenar e processar dados institucionais;
- Reduzir o intervalo de tempo entre a disponibilização das atualizações tecnológicas pelo mercado e a efetiva utilização pela instituição;
- Proporcionar o desenvolvimento e a sustentação de soluções que suportem os processos de trabalho da instituição;
- Proporcionar o desenvolvimento e a sustentação de soluções disruptivas na instituição;
- Otimizar a contratação de licenças dos softwares regidos pela portarias supracitadas.

Linhas bases e metas de benefício/resultado esperado:

- Maior disponibilidade dos sistemas;
- Maior frequência em atualização tecnológica;
- Mitigar riscos com infraestrutura física de apoio aos datacenters.

2. Escopo

O escopo desse documento se aplica às contratações de software e serviço de computação em nuvem estabelecidos na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 e regidos pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 e suas revisões. Os termos utilizados neste documento são os mesmos definidos nas portarias supracitadas.

3. Definições

Para o uso de nuvem pública, a organização adota os seguintes princípios e definições:

- Nuvem Pública: Serviços de computação em nuvem fornecidos por terceiros em ambientes compartilhados, incluindo armazenamento, processamento, banco de dados, redes e outros serviços.
- Dado Pessoal: Qualquer informação relacionada a uma pessoa natural identificada ou identificável, conforme definido pela LGPD (Lei Geral de Proteção de Dados).
- Dado Sensível: Dado pessoal sobre origem racial, religiosa, opinião política, saúde, genética, entre outros dados que exigem tratamento diferenciado.

- Segurança e Privacidade: Garantir que os dados sejam armazenados de forma segura, respeitando a confidencialidade e privacidade.
- Conformidade Legal: Cumprir as diretrizes da LGPD e normativas governamentais relacionadas ao armazenamento e tratamento de dados.
- Minimização de Dados: Limitar o armazenamento de dados ao necessário para a finalidade específica, reduzindo riscos.
- Transparência e Responsabilidade: Assegurar que as atividades relacionadas ao uso de nuvem pública sejam transparentes e que todas as partes envolvidas compreendam suas responsabilidades.
- Localização dos dados: Refere-se a localização geográfica (país, estado ou cidade) onde os dados são armazenados.

4. Diretrizes Gerais

4.1. Das necessidades do negócio

4.1.1. são elegíveis para utilização em nuvem:
- máquinas virtuais;
- sistemas web;
- armazenamento de arquivos;
- banco de dados;
- serviços de e-mail;
- softwares de produtividade;
- serviço de inteligência artificial;
- virtualização de desktops;
- serviços de autenticação;
- outros serviços de TI com capacidade técnica ou equivalente em nuvem

4.1.2. São condições mínimas necessárias para utilização do serviço em nuvem;
- disponibilidade e estabilidade de internet nos campus ou reitoria;
- largura de banda e latência suficientes nos campus ou reitoria;

4.2. Modelo de serviço e implementação

4.2.1. No âmbito da instituição fica definido o modelo de implementação híbrido, sendo composto por Nuvem Pública, Nuvem privada contratada ou do próprio órgão.

4.2.2. A instituição poderá usar quaisquer modelos de serviço em nuvem disponíveis, como IaaS, PaaS, SaaS ou outros que venham a ser disponibilizados pelos fornecedores.

4.3. Escolha de Provedores

4.3.1. Somente provedores de nuvem pública que atendam aos requisitos de segurança, privacidade e conformidade com a LGPD, Marco Civil da Internet e normas de segurança do governo federal (como o e-PING e IN 4/2020) devem ser utilizados.

4.3.2. Provedores devem assegurar a proteção de dados pessoais e sensíveis e disponibilizar relatórios de auditoria sobre conformidade e segurança.

4.3.3. Devem ser considerados provedores de serviços de grande relevância no mercado global ou provido por empresa pública, preferencialmente com amplo catálogo de serviços.

4.3.4. Os provedores de serviço devem ter infraestrutura e representantes legais em território brasileiro.

4.3.5. A instituição poderá solicitar demonstração, na fase de planejamento, desde que as pessoas externas envolvidas na atividade assinem termo de confidencialidade e com a garantia de exclusão total dos dados após o término do período por parte do fornecedor;

4.3.6. A equipe técnica de contratação poderá definir critérios de desempenho durante a fase de demonstração;

4.3.7. Novos provedores de serviços devem possuir compatibilidade com os serviços em nuvem pré-existentes na instituição;

4.3.8. Todo o provisionamento de serviço em nuvem deve priorizar a interoperabilidade de sistemas e mitigar a dependência tecnológica do provedor de serviço sempre que possível;

4.3.9. Realizar análise de risco de contratação e operação em nuvem;

4.4. Requisitos de Segurança do Provedor de Nuvem

4.4.1. Somente provedores de nuvem que cumpram os requisitos de segurança definidos na IN n.º 5, de 30 de agosto de 2021, incluindo a manutenção de controles de acesso e proteção de dados, poderão ser contratados.

4.4.2. O provedor deve disponibilizar auditorias periódicas e relatórios de conformidade para avaliação do órgão contratante, assegurando que os dados sejam protegidos e monitorados.

4.5. Classificação e Proteção de Dados

4.5.1. Todos os dados armazenados e processados em ambientes de nuvem devem ser classificados segundo a sua sensibilidade e valor, conforme as diretrizes da Política de Segurança da Informação do órgão ou entidade.

4.5.2. Dados sensíveis e informações classificadas devem ser protegidos por medidas adicionais de segurança, incluindo criptografia e controles de acesso.

4.5.3. A instituição deve ter política ou normativo com a identificação e classificação dos dados, controle de acesso, gerenciamento de configuração e quando for o caso, monitoramento das atividades em nuvem;

- Enquanto a política não for criada, todos os dados armazenados pela instituição ficam elegíveis para armazenamento em nuvem, independente de sua classificação, desde que o provedor de serviço esteja aderente aos normativos legais da LGPD, Marco Civil da Internet ou correspondentes;

4.6. Localização dos Dados

4.6.1. De acordo com a IN n.º 5/2021, é obrigatório que pelo menos uma cópia dos dados sensíveis seja mantida em território nacional.

4.6.2. A transferência e o armazenamento de dados fora do Brasil devem estar em conformidade com a Lei Geral de Proteção de Dados (LGPD), e é necessário garantir que a segurança dos dados seja equivalente àquela oferecida em território nacional.

4.7. Requisitos de Armazenamento

4.7.1. Dados pessoais devem ser armazenados em conformidade com a LGPD, com garantias de que o provedor de nuvem utiliza mecanismos adequados de criptografia e controle de acesso.

4.8. Controle de Acesso e Autenticação

4.8.1. Somente usuários autorizados poderão acessar dados armazenados na nuvem, e o acesso deverá ser limitado conforme o princípio de privilégio mínimo.

4.8.2. O acesso aos dados e sistemas em nuvem deve ser concedido apenas a usuários autorizados, com base no princípio do menor privilégio.

4.8.3. A autenticação multifator é obrigatória para o acesso a sistemas que contenham dados sensíveis ou classificados.

4.8.4. Os logs de acesso ao ambiente de nuvem devem ser mantidos por pelo menos 03 (três) anos, como previsto pela normativa, para assegurar a rastreabilidade e o monitoramento de ações no ambiente de nuvem.

4.9. Criptografia e Proteção de Dados

4.9.1. Dados em repouso e em trânsito devem ser criptografados, especialmente quando se tratam de dados pessoais e sensíveis.

4.9.2. Os mecanismos de criptografia e segurança devem ser revistos e atualizados regularmente para proteger as informações contra ameaças emergentes.

4.10. Retenção e Exclusão de Dados

4.10.1. Os dados devem ser armazenados pelo tempo mínimo necessário para a finalidade estabelecida e, posteriormente, excluídos ou anonimizados.

4.10.2. Ao término do contrato com o provedor de nuvem, deve-se garantir a exclusão de todos os dados da organização no ambiente do provedor, com comprovação da exclusão.

4.11. Transferência Internacional de Dados

4.11.1. Para dados armazenados em nuvens com servidores fora do Brasil, deve-se assegurar conformidade com as diretrizes da LGPD quanto à transferência internacional de dados.

4.11.2. Garantias contratuais de proteção de dados pessoais devem ser firmadas com os provedores, de acordo com a legislação de proteção de dados no país de destino.

4.12. Monitoramento e Gestão de Incidentes

4.12.1. Devem ser realizados monitoramento e auditorias regulares para avaliar a conformidade com as políticas de segurança e proteção de dados.

4.12.2. O provedor de nuvem deve permitir auditorias de segurança da informação e fornecer logs de acesso aos dados armazenados para fins de rastreabilidade.

4.12.3. O ambiente de nuvem deve dispor de monitoramento contínuo de performance do ambiente, e fornecer meios para identificar, avaliar e responder a incidentes de segurança da informação.

4.12.4. Em caso de incidentes que possam comprometer a segurança dos dados, o provedor de nuvem deverá notificar imediatamente os respectivos agentes internos da instituição, permitindo a adoção de medidas corretivas e mitigadoras.

4.12.5. Todos os incidentes e violações devem ser documentados e relatados aos agentes responsáveis pela segurança da informação, ao encarregado de proteção de dados (DPO) do órgão e à ETIR (Equipe de Tratamento de Incidente e Resposta) ou equivalente.

4.13. Auditorias e Avaliações Periódicas

4.13.1. O órgão deve realizar auditorias de segurança e conformidade periodicamente para garantir que o provedor de nuvem está atendendo aos requisitos de segurança da IN n.º 5/2021 e das políticas internas.

4.13.2. A avaliação deve incluir a verificação de medidas de segurança física, controle de acesso lógico, conformidade com a LGPD e outros requisitos legais.

4.14. Notificação de Incidentes

4.14.1. Incidentes de segurança envolvendo dados pessoais na nuvem devem ser comunicados imediatamente por meios oficiais (e-mail ou telefone) aos agentes responsáveis pela segurança da informação, ao encarregado de proteção de dados (DPO) do órgão e à ETIR ou equivalente.

4.14.2. Provedores devem garantir suporte para a notificação imediata de incidentes e colaborar para mitigar os impactos e informar as autoridades conforme exigido por legislação vigente.

4.15. Termos Contratuais e Conformidade

4.15.1. O contrato com o provedor de nuvem deve incluir cláusulas específicas sobre a segurança da informação, a proteção de dados e o cumprimento da IN n.º 5/2021.

4.15.2. O provedor deve assinar termos de confidencialidade (NDA) e se comprometer a garantir a proteção dos dados do órgão, proibindo qualquer uso dos dados fora das finalidades estipuladas pelo contratante.

5. Responsabilidades

5.1. Órgãos e Entidades Contratantes

5.1.1. Garantir que todos os requisitos de segurança estabelecidos pela IN n.º 5/2021 sejam cumpridos no processo de contratação e utilização de serviços de nuvem.

5.1.2. Realizar a classificação dos dados e definir controles de segurança compatíveis com a criticidade da informação.

5.1.3. Compete à Pró-reitoria de Governança, Engenharia, Tecnologia e Ingresso, juntamente com à Pró-reitoria de Administração a realização de processo de contratação de serviços em nuvem, seguindo a legislação vigente à época.

5.1.4. a instituição deve fornecer cursos e atividades de transferência de conhecimento para os servidores envolvidos na gestão dos serviços em nuvem, preferencialmente as aquisições de soluções em nuvem devem incluir a transferência de conhecimento pelo fornecedor da solução;

5.2. Usuários e Colaboradores

5.2.1. Garantir a conformidade com esta política no uso de nuvem pública e relatar qualquer comportamento suspeito ou violação de dados.

5.2.2. Utilizar os serviços de nuvem em conformidade com as diretrizes de segurança da informação e da POSIC da instituição.

5.2.3. Reportar qualquer incidente ou anomalia detectada nos sistemas de nuvem ao responsável pela segurança da informação.

5.2.4. a área de negócio requisitante de licença de software de uso específico ficará responsável pela licença e pelo gerenciamento dos usuários;

- Exemplo: Software de CAD ou edição de imagens possuem características técnicas e condições de uso de licenças específicos de conhecimento dos utilizadores, sendo assim estes devem, ao requisitar, elencar todas as especificações técnicas e requisitos legais da contratação.

5.3. Provedor de Nuvem

5.3.1. Garantir que suas práticas estejam de acordo com as exigências da LGPD e normativas do governo brasileiro, mantendo a segurança e privacidade dos dados.

5.3.2. Proteger os dados armazenados em conformidade com as exigências de segurança e privacidade estabelecidas pelo contratante.

5.3.3. Disponibilizar mecanismos para auditorias de conformidade e manter uma comunicação transparente com o órgão em casos de incidentes.

5.4. Departamento de TI

5.4.1. Avaliar e monitorar o uso de nuvem pública, implementando medidas técnicas para proteger dados e acessos.

5.4.2. Revisar periodicamente os provedores de nuvem e realizar auditorias para garantir que estejam em conformidade com as políticas e normativas.
5.4.3. Estabelecer critérios técnicos para contratação dos serviços;
5.4.4. Manter um plano de retorno em estrutura on-site;
5.4.5. Criar plano de migração dos sistemas e serviços para nuvem;
5.4.6. Gerenciar o serviço de nuvem, podendo subdelegar a Coordenação de Tecnologia da Informação do campus ou usuário requisitante, quando necessário.

5.5. Encarregado de Proteção de Dados (DPO)

5.5.1. Supervisionar o cumprimento da LGPD no uso da nuvem e atuar como ponto de contato para autoridades e titulares de dados.

5.6. Gestor de Segurança da Informação

5.6.1. Apoiar e supervisionar na aplicação de medidas de segurança da informação de acordo com as boas práticas e recomendações da Política de Segurança da Informação.

6. Estratégia de migração

6.1. A migração dos serviços será realizada de maneira escalonada, por prioridade de serviço e interdependência, começando primeiro pelos sistemas de menor dependência;
6.2. O cronograma de migração deverá ser elaborado considerando o orçamento disponibilizado para consumo de serviços em nuvem;
6.3. Os dados devem ser transferidos com ferramenta que garanta segurança
6.4. A migração será considerada completa após a realização de testes dos ambientes;
6.5. Os serviços serão migrados como estão (as-is) quando não houver ainda capacidade técnica para realizar adaptações nativas de tecnologia em nuvem;

7. Estratégia de saída

7.1. Nas circunstância que ocorram necessidade de saída, como por exemplo, custos, requisitos regulatórios ou mudanças de políticas de segurança de informação, as seguintes ações devem ser consideradas:
7.1.1. Análise de dependências;
7.1.2. Dependências entre sistemas, aplicativos e dados na nuvem;

7.1.3. interconexões críticas que possam impactar a migração de volta ao on-premisse
7.1.4. Avaliação de portabilidade;
7.1.5. Portabilidade das soluções e dados armazenados na nuvem, considerando padrões e evitando bloqueios em virtude de fornecedores;
7.1.6. Utilização de ferramentas de migração e backup que suportem a transferência dos dados durante o retorno ao on-premisse;

7.2. A instituição manterá infraestrutura própria mínima para acomodar ao menos uma cópia dos sistemas institucionais provisionados em nuvem

8. Revisão e Atualização

8.1. A presente política deve ser revisada anualmente ou sempre que houver alterações na legislação, ou em normativas aplicáveis, para garantir a contínua conformidade e proteção dos dados armazenados em nuvem.

9. Referências

IFSP. Política de Uso de serviços em nuvem do IFSP: Em desenvolvimento.
IFC. Estratégica de Uso de serviços em nuvem do IFC: Em desenvolvimento.
IFES. Normativa de serviços em nuvem do IFES. Disponível em: https://prodi.ifes.edu.br/images/stories/Prodi/DRTI/Aprovada_-_Normativa_-_TI_-_Servi%C3%A7o_de_Computa%C3%A7%C3%A3o_em_Nuvem.pdf. Acesso em: 14 jan. 2025.
BRASIL. Receita Federal do Brasil. Resolução de nuvem da Receita Federal do Brasil. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=138694. Acesso em: 14 jan. 2025.
IFTO. Estratégia de Nuvem do IFTO. Disponível em: https://portal.ifto.edu.br/acesso-a-informacao/seguranca-da-informacao/documentos-lgpd-ifto/EstrategiaNuvem.pdf. Acesso em: 14 jan. 2025.
IFTO. Uso seguro de nuvem do IFTO. Disponível em: https://portal.ifto.edu.br/acesso-a-informacao/seguranca-da-informacao/documentos-lgpd-ifto/USCN.pdf. Acesso em: 14 jan. 2025.
IFSC. Plano de software e computação em nuvem do IFSC. Disponível em: https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=3641120&key=e4099251477dff9bbffade1d062dd28f. Acesso em: 14 jan. 2025.
BRASIL. Governo Federal. Estratégia de Nuvem do Governo Federal. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/copy_of_legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 14 jan. 2025.
UFRGS. TERMO DE USO – NUVEM UFRGS. Disponível em: https://www.ufrgs.br/documentacaoti/termo-de-uso-e-politica-de-privacidade-nuvem-ufrgs/. Acesso em: 14 jan 2025.

BRASIL. INSTRUÇÃO NORMATIVA N.º 5, DE 30 DE AGOSTO DE 2021. 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.
BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados.
BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

PORTARIA NORMATIVA - ANEXOS Nº 4/2025 - ASSINST/REI (11.01.18.00.65)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/05/2025 10:57)
RUDINEI KOCK EXTERCKOTER
REITOR

Visualize o documento original em https://sig.ifc.edu.br/documentos/ informando seu número: ***4****, ano:* ***2025****, tipo:* ***PORTARIA NORMATIVA - ANEXOS****, data de emissão:* ***05/05/2025*** *e o código de verificação:* ***e586c49a3c***