FIOCRUZ

Coordenação-Geral de Gestão de Tecnologia de Informação

PORTARIA Nº 7, de 11 de setembro de 2025

A Coordenação-Geral de Gestão de Tecnologia da Informação e Comunicação da Fundação Oswaldo Cruz - COGETIC, no uso das suas atribuições, estabelecidas pelo Decreto nº 8.932, de 14 de dezembro de 2016 - Estatuto da Fiocruz,

RESOLVE:

1.0 – PROPÓSITO

Esta Portaria tem como objetivo aprovar, no âmbito da Fundação Oswaldo Cruz – Fiocruz, a Política de Uso do Centro de Dados para Computação em Nuvem. A política estabelece normas, diretrizes e responsabilidades relacionadas à utilização, gestão e segurança da infraestrutura tecnológica disponibilizada, visando assegurar a continuidade dos serviços, a integridade das informações e o alinhamento às diretrizes institucionais e às orientações do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

2.0 – REGRAS DE USO

SEÇÃO I
ESCOPO DO CENTRO DE DADOS PARA COMPUTAÇÃO EM NUVEM

Art. 1 O Centro de Dados para Computação em Nuvem tem como finalidade oferecer, preferencialmente, os modelos de Plataforma como Serviço (PaaS) ou Software como Serviço (SaaS) às unidades da Fundação Oswaldo Cruz (Fiocruz), em substituição ao modelo de Infraestrutura como Serviço (IaaS), conforme disposto nos Artigos 6 e 9º da Portaria da Diretoria Executiva nº 24, de 8 de outubro de 2024.

Art. 2 O modelo de implementação adotado é baseado na abordagem de Nuvem Híbrida, compreendendo infraestrutura de nuvem pertencente à Fiocruz e suas unidades, incluindo serviços de hospedagem de portais e sites na nuvem institucional, bem como serviços hospedados em nuvens públicas e nuvem soberana.

SEÇÃO II
DISPOSIÇÕES GERAIS

Art. 3 Esta Política estabelece as responsabilidades relativas à administração do Centro de Dados da Fiocruz e ao seu uso pelas Unidades da Fundação.

Art. 4 A administração do Centro de Dados é atribuição específica da Coordenação-Geral de Tecnologia da Informação e Comunicação (COGETIC/Fiocruz).

Art. 5 A administração e a atualização dos serviços ofertados observarão as seguintes disposições:

I. Os serviços ofertados pela COGETIC e hospedados na Nuvem Fiocruz são de responsabilidade da própria COGETIC/Fiocruz;

II. Os serviços hospedados no pool de recursos das Unidades na Nuvem Fiocruz são de responsabilidade das respectivas Unidades, conforme as políticas e diretrizes estabelecidas pela COGETIC;

III. As Unidades detentoras de pool de recursos devem manter atualizado o inventário dos servidores e serviços sob sua gestão, conforme orientações da COGETIC;

IV. As Unidades são integralmente responsáveis pela manutenção, atualização e funcionamento adequado dos serviços sob sua gestão, incluindo plug-ins, temas, bibliotecas, extensões e demais dependências, devendo garantir que os sistemas e conteúdos estejam atualizados e em conformidade com as diretrizes institucionais e da COGETIC, corrigindo falhas em tempo hábil para evitar impactos à disponibilidade e à segurança;

V. O suporte técnico da COGETIC deve ser acionado exclusivamente para questões relacionadas à infraestrutura de hospedagem, não abrangendo intervenções nos sistemas ou conteúdos gerenciados pelas Unidades;

VI. Cabe às Unidades realizar o monitoramento periódico de desempenho e uso dos serviços, adotando medidas preventivas sempre que necessário e reportando à COGETIC conforme as políticas estabelecidas.

Art. 6 Para fins desta Política, consideram-se as seguintes definições:

I. Centro de Dados para Computação em Nuvem (Data Center): ambiente destinado à concentração de equipamentos de processamento e armazenamento de dados da organização, projetado para oferecer elevado nível de segurança. Abriga servidores, ativos de rede (como switches e roteadores) e bancos de armazenamento (*storages*), sendo capaz de processar grandes volumes de informação;

II. Sala Cofre: ambiente que atende aos requisitos de segurança física para proteção de equipamentos de tecnologia da informação, devendo possuir certificação conforme a norma ABNT NBR 15.247 (Unidades de armazenagem segura – Salas-cofre e cofres para hardware – Classificação e métodos de ensaio de resistência ao fogo), norma EN 1047-2 (Unidades de armazenamento seguro – Classificação e métodos de teste de resistência ao fogo para salas de dados e contêineres de dados), ou normas similares reconhecidas por organismos acreditadores internacionais;

III. Órgão Seccional: denominação atribuída à Coordenação-Geral de Gestão em Tecnologia da Informação e Comunicação – COGETIC, responsável pela gestão do Centro de Dados para Computação em Nuvem;

IV. Órgão Correlato: denominação atribuída às Unidades da Fiocruz que utilizam os serviços do Centro de Dados para Computação em Nuvem;

V. Portal de Autosserviço: interface web para interação com os serviços disponibilizados na nuvem, semelhante a uma “loja online”. É acessível por meio de navegadores de internet (como Chrome, Edge ou Firefox), permitindo que os recursos sejam gerenciados pelos Órgãos Correlatos e acessados por usuários devidamente autorizados;

VI. *Templates* de Máquinas Virtuais: modelos padronizados de máquinas virtuais, configurados conforme o tipo de serviço a ser implementado (ex.: servidor web, servidor de banco de dados). Contêm o

conjunto mínimo de softwares necessários para início da operação, sendo a instalação, gestão e atualização dos demais componentes responsabilidade dos Órgãos Correlatos;

VII. Central de Serviços: sistema institucional de requisições utilizado para solicitação dos serviços da Nuvem Fiocruz, disponível em https://centraldeservicos.fiocruz.br.

SEÇÃO III
DA POLÍTICA DE USO DO CENTRO DE DADOS PARA COMPUTAÇÃO EM NUVEM

Art. 7 A Política de Uso do Centro de Dados para Computação em Nuvem tem como objetivo estabelecer parâmetros para a gestão dos serviços da infraestrutura tecnológica da Fiocruz, promovendo sua qualidade e estabilidade, além de regular as relações entre a COGETIC e as Unidades da Fundação, com base nos seguintes princípios:

I. Reconhecimento do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, conforme determinado pelo Decreto nº 7.579, de 11 de outubro de 2011, da Presidência da República, que atribui ao Órgão Seccional (COGETIC), nos termos do art. 7, inciso I, a responsabilidade de cumprir e fazer cumprir, por meio de políticas, diretrizes, normas e projetos seccionais, as orientações emanadas do Órgão Setorial do SISP ao qual está vinculado. Ao Órgão Correlato, conforme o art. 8, inciso I do mesmo Decreto, cabe subsidiar o Órgão Seccional no cumprimento das políticas, diretrizes e normas gerais relativas ao SISP;

II. Promoção da cooperação entre as áreas e incentivo à integração institucional, em conformidade com os valores da Fiocruz expressos em sua Carta de Serviço ao Cidadão.

Art. 8 Os serviços do Centro de Dados para Computação em Nuvem são gerenciados de forma compartilhada, sendo parte da gestão realizada pelo Órgão Seccional (COGETIC) e parte pelos Órgãos Correlatos, sob coordenação e supervisão macro da COGETIC.

Art. 9º A COGETIC é responsável pela manutenção desta Política, pela recepção de contribuições das Unidades da Fiocruz e pela garantia da coesão técnica do documento.

Art. 10 º Os atendimentos relacionados aos serviços do Centro de Dados para Computação em Nuvem deverão observar as seguintes disposições:

I. As solicitações de atendimento devem ser formalmente registradas por meio da Central de Serviços;

II. Em caso de indisponibilidade da Central de Serviços, as Unidades poderão encaminhar suas solicitações diretamente à Central por meio do WhatsApp, pelo número (21) 3836-2132;

III. O catálogo de serviços, bem como os respectivos acordos de nível de serviço (SLA), está disponível na Central de Serviços.

Art. 11 O serviço de backup no âmbito do Centro de Dados para Computação em Nuvem observará as seguintes disposições:

I. A COGETIC é responsável pela realização das cópias de segurança dos servidores virtuais de produção cedidos para hospedagem de serviços das Unidades;

II. A Unidade Correlata deverá indicar os serviços que devem ser incluídos nas rotinas de backup. Serão realizados apenas backups de máquinas de produção; máquinas de homologação e testes não serão contempladas nessas rotinas;

III. A COGETIC realizará cópias de segurança exclusivamente dos servidores virtuais que hospedam serviços providos pela própria COGETIC. Serviços não ofertados pela COGETIC deverão ser migrados para a plataforma da Coordenação, mediante solicitação formal da Unidade por meio da Central de Serviços;

IV. A COGETIC será responsável pela execução de operações de restauração dos serviços em casos de indisponibilidade causada por falhas físicas ou problemas com ferramentas de virtualização. Os tempos de resposta para início do atendimento estão definidos no catálogo de serviços da COGETIC. Após iniciado o atendimento, o tempo médio de recuperação é de 500 GB/h;

V. Toda solicitação de restauração deverá ser formalizada por meio da Central de Serviços e direcionada à equipe da COGETIC;

VI. No momento da criação de novos serviços, a Unidade Correlata deverá solicitar à COGETIC a inclusão do serviço na rotina de backup, conforme planejamento prévio;

VII. A COGETIC se exime de qualquer responsabilidade quanto à realização de backups caso a Unidade não observe as recomendações estabelecidas nesta Política.

Art. 12 A COGETIC é responsável pela macrogestão do ambiente do Centro de Dados para Computação em Nuvem, cabendo-lhe as seguintes atribuições:

I. Administrar o Centro de Dados para Computação em Nuvem, incluindo a infraestrutura tecnológica necessária e a definição das regras de uso, alinhadas às recomendações do SISP, às normas legais, às orientações dos órgãos de controle e às necessidades dos Órgãos Correlatos, assegurando o cumprimento dessas regras;

II. Disponibilizar acesso ao Portal de Autosserviço aos Órgãos Correlatos que possuam acesso direto a um pool de recursos, permitindo-lhes o gerenciamento dos recursos disponíveis;

III. Realizar análise e resolução avançada de problemas técnicos nos servidores do Centro de Dados;

IV. Oferecer suporte especializado, contribuindo para a estabilidade e eficiência do Centro de Dados, excetuando os servidores que estejam sob administração direta das Unidades;

V. Criar, manter e prestar suporte técnico aos serviços cedidos para hospedagem de soluções dos Órgãos Correlatos;

VI. Administrar os servidores e fornecer as credenciais de acesso aos serviços pelas Unidades;

VII. Criar e atualizar regularmente os templates de máquinas virtuais disponibilizados no Portal de Autosserviço, contendo apenas os recursos em suas versões mais atuais;

VIII. Avaliar a necessidade de criação de novos templates de servidores virtuais customizados, conforme demandas dos Órgãos Correlatos, desde que os requisitos não estejam contemplados nos modelos existentes e estejam em conformidade com as diretrizes de Segurança da Informação previstas nesta Política;

IX. Garantir que todas as plataformas mantidas na Nuvem Fiocruz sejam atualizadas diariamente;

X. Avaliar as solicitações recebidas dos Órgãos Correlatos, por meio da Central de Serviços, referentes às operações no Centro de Dados para Computação em Nuvem, atendendo-as quando não representarem risco à integridade dos serviços e estiverem em conformidade com a legislação vigente, jurisprudência, normas, regulamentos e políticas aplicáveis;

XI. Informar aos Órgãos Correlatos, com antecedência mínima de 3 (três) dias, sobre interrupções técnicas ou manutenções que demandem mais de 6 (seis) horas de duração e/ou que possam comprometer a operacionalidade dos serviços, exceto em casos de urgência, assim considerados aqueles que coloquem em risco o funcionamento regular da infraestrutura tecnológica;

XII. Atualizar os procedimentos técnicos dos serviços ofertados, sem necessidade de aviso prévio, desde que tais atualizações não impactem o funcionamento dos serviços prestados.

Art. 13 Compete às áreas de Tecnologia da Informação e Comunicação (TIC) dos Órgãos Correlatos as seguintes responsabilidades:

I. Administrar os recursos cedidos pelo Órgão Seccional (COGETIC), mantendo as aplicações sempre atualizadas quanto às versões e correções de segurança, em estrita conformidade com as políticas e diretrizes estabelecidas pela COGETIC;

II. Gerenciar todas as licenças de software necessárias ao funcionamento dos serviços hospedados na infraestrutura da COGETIC, sendo esta responsabilidade exclusiva dos Órgãos Correlatos. O Órgão Seccional (COGETIC/Fiocruz) não se responsabiliza pela aquisição, ativação, uso indevido ou utilização de licenças não originais;

III. Impedir a instalação de softwares não originais e monitorar eventuais instalações indevidas. Caso seja identificado o uso de tais softwares, a Unidade Correlata será notificada e o serviço correspondente será excluído. Incidentes dessa natureza devem ser reportados à COGETIC;

IV. Realizar a guarda adequada das credenciais de acesso (login e senha) aos serviços, não cabendo à COGETIC qualquer responsabilidade pelo uso indevido dessas informações;

V. Solicitar, por meio da Central de Serviços, ajustes no pool de recursos destinados aos serviços, cientes de que tais solicitações estarão sujeitas à análise técnica e orçamentária da equipe da COGETIC;

VI. Planejar previamente a inclusão ou expansão de serviços, respeitando os limites dos recursos disponibilizados;

VII. Cumprir todas as restrições e seguir as recomendações estabelecidas na Política de Segurança da Informação da Fiocruz vigente, bem como nas diretrizes da COGETIC. O descumprimento das ações de segurança será passível de sanções previstas nesta Política;

VIII. Implementar autenticação única (SSO) com múltiplos fatores de autenticação (MFA) em seus sistemas e serviços, conforme padrões e orientações da COGETIC, visando prevenir o vazamento de credenciais;

IX. Manter todas as aplicações atualizadas ou migradas para novos ambientes dentro dos prazos estabelecidos pela COGETIC, evitando a obsolescência dos recursos computacionais;

X. Implementar, configurar, manter e monitorar soluções de segurança que mitiguem ameaças e vulnerabilidades nos ambientes computacionais utilizados, em consonância com as políticas e ferramentas recomendadas pela COGETIC;

XI. Assegurar a integração entre sistemas e serviços que enviem e-mails com o serviço institucional de SMTP Seguro, fornecido e mantido pela COGETIC;

XII. Impedir o uso dos serviços disponibilizados na Nuvem Fiocruz para envio de mensagens eletrônicas indesejadas (spam), publicidades não solicitadas, e-mails não autorizados ou qualquer outro tipo de comunicação que possa gerar reclamações de destinatários, instituições ou órgãos de combate à prática de SPAM;

XIII. Adotar práticas rotineiras de monitoramento para evitar o bloqueio do IP válido da Fiocruz por órgãos ou organismos antispam;

XIV. Abster-se de armazenar, nos recursos disponibilizados, conteúdos não relacionados à atividade fim da Fiocruz ou que possam comprometer o funcionamento da Nuvem Fiocruz;

Parágrafo único. Qualquer incidente de segurança deverá ser imediatamente notificado à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Fiocruz (EPTRIC), por meio do e-mail: csirt@ fiocruz.br.

Art. 14 O descumprimento de qualquer disposição da Política de Uso da Nuvem Fiocruz será objeto de análise prévia, com o objetivo de identificar se a violação ocorreu de forma intencional.

Art. 15 Caso seja constatado que o descumprimento foi intencional, o responsável estará sujeito à aplicação das medidas administrativas e legais cabíveis.

Art. 16 Esta Política correlaciona-se com as seguintes normas legais, sem se limitar a elas:

a) Lei Federal nº 8.159, de 8 de janeiro de 1991 – Dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

b) Lei Federal nº 9.609, de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programas de computador;

c) Lei Federal nº 9.610, de 19 de fevereiro de 1998 – Dispõe sobre o Direito Autoral;

d) Lei Federal nº 9.279, de 14 de maio de 1996 – Dispõe sobre Marcas e Patentes;

e) Lei Federal nº 10.406, de 10 de janeiro de 2002 – Institui o Código Civil;

f) Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Institui o Código Penal;

g) Lei Federal nº 9.983, de 14 de julho de 2000 – Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal;

h) Lei Federal nº 12.737, de 30 de novembro de 2012 – Dispõe sobre a tipificação criminal de delitos informáticos;

i) Lei Federal nº 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

j) Decreto nº 1.171, de 22 de junho de 1994 – Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

Art. 17 Caso o descumprimento das regras previstas nesta Política implique em prejuízo à Fiocruz ou a terceiros, de qualquer natureza, imediata ou iminente, os serviços poderão ser suspensos até que as providências corretivas sejam adotadas pelo Órgão Correlato.

SEÇÃO V
SEGURANÇA DA INFORMAÇÃO

Art. 18 A COGETIC é a responsável principal pela proteção do ambiente computacional da Fiocruz, por meio da implementação de medidas robustas de segurança da informação, alinhadas às diretrizes institucionais. Para tanto, por meio de sua Coordenação de Segurança da Informação, são atribuídas as seguintes responsabilidades:

I. Proteção do Ambiente de Tecnologia: Estabelecer políticas de controle de acesso e definir diretrizes gerais de segurança para os ativos hospedados no Centro de Dados (Datacenter), assegurando a integridade, confidencialidade e disponibilidade das informações;

II. Macrogestão da Segurança da Informação: Realizar a gestão estratégica do ambiente computacional da Fiocruz, fornecendo orientações técnicas e normativas para a operação da Nuvem Fiocruz.

Art. 19 A COGETIC é responsável por estabelecer e supervisionar a política de fortalecimento (*hardening*) de todo o ambiente computacional da Fiocruz, assegurando a proteção dos sistemas e serviços. O processo de hardening deverá ser conduzido conforme as diretrizes da COGETIC e observar as seguintes responsabilidades:

I. Cabe à Unidade realizar o *hardening* dos sistemas e serviços não disponibilizados pela COGETIC antes

de sua entrada em produção;

II. Cabe à Unidade manter um processo contínuo de *hardening*, independentemente da origem do sistema operacional ou serviço;

III. Cabe à Unidade revisar os protocolos de rede utilizados e desativar aqueles que não estejam em uso;

IV. Cabe à Unidade utilizar as portas TCP/UDP padrão designadas para cada serviço;

V. Cabe à Unidade revisar continuamente os serviços, aplicativos e pacotes instalados, desativando aqueles que não sejam necessários;

VI. Cabe à Unidade revisar continuamente as contas e grupos de usuários, removendo aqueles que não estejam em uso;

VII. Cabe à COGETIC aplicar boas práticas de configuração em dispositivos diversos, incluindo, mas não se limitando, a sistemas operacionais, serviços e componentes de rede, como switches e roteadores;

VIII. Cabe à Unidade aplicar boas práticas de *hardening* disponíveis no mercado, conforme orientações da COGETIC, utilizando fontes confiáveis como sites de fabricantes e listas reconhecidas de segurança;

IX. No caso de sistemas, serviços e aplicativos legados que não possam ser submetidos ao processo de *hardening*, cabe à Unidade garantir a implementação de controles compensatórios que assegurem níveis adequados de segurança, incluindo a instalação de antivírus ou outros softwares recomendados pela COGETIC;

X. Cabe à Unidade, sempre que possível, utilizar ferramentas que verifiquem a base de pacotes, serviços e aplicações instaladas, correlacionando-as com informações de vulnerabilidades publicadas;

XI. Cabe à Unidade garantir a instalação nos servidores dos agentes de segurança oficiais disponibilizados pela área de segurança da informação.

Art. 20 A COGETIC é responsável por gerenciar e supervisionar a política de atualizações em toda a infraestrutura e nos serviços hospedados, visando garantir a segurança e o desempenho contínuo. Para isso, são estabelecidas as seguintes responsabilidades:

I. Cabe à COGETIC implementar um processo de gestão de mudanças para intervenções no Centro de Dados da Fiocruz;

II. Cabe à Unidade implementar um processo de gestão de mudanças para intervenções nos serviços sob sua responsabilidade, em conformidade com as diretrizes da COGETIC;

III. Cabe à COGETIC disponibilizar repositórios para os sistemas operacionais ofertados como *templates*;

IV. Cabe à Unidade manter todos os recursos atualizados (sistema operacional, firmware, plug-ins, etc.), independentemente da forma de atualização (versão, upgrade, patch, hotfix, etc.), seguindo as orientações da COGETIC;

V. Cabe à Unidade manter um ambiente de homologação, com o objetivo de avaliar os possíveis impactos de atualizações no ambiente de produção;

VI. Cabe à COGETIC informar, com a máxima antecedência possível, as atualizações que possam impactar serviços transversais ofertados às Unidades;

VII. COGETIC e Unidades devem, em conjunto, garantir processos internos de implantação, testes e gerenciamento de atualizações;

VIII. COGETIC e Unidades devem, em conjunto, assegurar a implementação de controles de segurança adequados para sistemas, serviços e aplicativos legados que não possam ser atualizados;

IX. COGETIC e Unidades devem, em conjunto, adotar soluções para gestão do ciclo de vida de seus sistemas

Art. 21 – Network Time Protocol – NTP

I. Cabe à Unidade sincronizar seus dispositivos de rede com a hora legal brasileira, por meio do serviço NTP da Fiocruz;

II. O serviço NTP da Fiocruz está disponível através do servidor: ntp.fiocruz.br.

Art. 22 – Monitoramento

I. Cabe à COGETIC monitorar toda a infraestrutura que compõe a Nuvem Fiocruz (Sala Cofre e Centro de Dados), visando garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações;

II. Cabe à Unidade monitorar os recursos e serviços hospedados em seu Centro de Dados Virtual, em conformidade com as diretrizes e ferramentas estabelecidas pela COGETIC;

III. O monitoramento realizado pela COGETIC deve permitir, no mínimo, o envio de notificações aos responsáveis pelos serviços nas Unidades;

IV. O monitoramento realizado pela COGETIC deve ocorrer sem impactos negativos ao desempenho do ambiente e dos serviços hospedados.

Art. 23 – Segmentação da Rede

I. Cabe à Unidade realizar estudo e planejamento quanto ao quantitativo de endereços IP necessários à manutenção de seus serviços, submetendo a solicitação formal e antecipada à COGETIC para análise;

II. Cabe à COGETIC analisar o pedido de cessão de novo bloco de endereçamento IP e avaliar sua viabilidade.

Art. 24 – Firewall

I. Nos casos em que a Unidade necessite implementar controles na borda da rede, deverá submeter pedido à COGETIC para configuração das regras no firewall de borda;

II. Cabe à Unidade documentar as configurações do firewall virtual sob sua responsabilidade.

Art. 25 – Gerência de Vulnerabilidades

I. Cabe à COGETIC e Unidades implementarem processo de gerenciamento de vulnerabilidades nos serviços sob sua responsabilidade;

II. Deve ser realizada, periodicamente, análises de vulnerabilidades em seus sistemas e serviços, em alinhamento com as diretrizes da COGETIC;

III. Caso a Unidade não disponha de ferramentas para essa análise, o Serviço de Segurança da Informação e Comunicações da COGETIC poderá ofertar o serviço mediante solicitação via Central de Serviços;

IV. Cabe à Unidade implementar, de forma imediata, os controles necessários para correção das vulnerabilidades identificadas e reportar à COGETIC as ações tomadas.

Art. 26 – IDS/IPS e Malware

I. Cabe à COGETIC analisar o tráfego de entrada e saída da Internet, incluindo o tráfego criptografado;

II. Cabe à COGETIC notificar a Unidade sobre comportamentos suspeitos identificados em seu ambiente;

III. Cabe à COGETIC monitorar o tráfego interno do ambiente virtualizado;

IV. Cabe à COGETIC implementar soluções de segurança contra malware, bem como sistemas de detecção e prevenção de intrusões (IDS/IPS) no ambiente virtualizado.

Art. 27 – Logs

I. A COGETIC mantém os registros (logs) dos equipamentos que compõem a infraestrutura da Nuvem Fiocruz (Nutanix), com o objetivo de assegurar rastreabilidade, diagnóstico de falhas e monitoramento operacional contínuo.

Art. 28 – Segurança de Perímetro

I. Cabe à COGETIC a gestão do Centro de Dados da Fiocruz, composto pelos seguintes componentes:

a) Sala Cofre: ambiente seguro e certificado para operações de Tecnologia da Informação;

b) Centro de Dados: conjunto de recursos destinados à conectividade, processamento e armazenamento de dados.

II. Cabe ao Serviço de Segurança da Informação e Comunicações da COGETIC:

a) Gerenciar o ambiente da Sala Cofre;

b) Realizar, ao menos uma vez ao ano, análises de riscos operacionais, de negócio e estruturais do Centro de Dados, com divulgação dos resultados à Câmara Técnica de Gestão e Desenvolvimento Institucional e às áreas de TIC correlatas;

c) Acompanhar as Unidades e equipes de manutenção durante visitas técnicas;

d) Administrar os contratos de manutenção do ambiente da Sala Cofre.

III. Cabe ao Serviço de Infraestrutura Tecnológica da COGETIC:

a) Gerenciar os recursos (equipamentos e serviços) do Centro de Dados;

b) Administrar os contratos de manutenção do Centro de Dados.

Art. 29 – Gestão de Incidentes de Segurança da Informação

I. Os incidentes de segurança da informação serão tratados conforme o Modelo de Gestão de Incidentes de Segurança da Informação e Comunicações da Fiocruz e outros normativos vigentes.

Art. 30 – Conformidade

I. Cabe à COGETIC conduzir análises de conformidade sobre o conjunto de recursos que compõem a Nuvem Fiocruz, com o objetivo de verificar a implementação dos controles de segurança requeridos;

II. A análise de conformidade deve ser realizada ao menos uma vez ao ano, com base nas diretrizes da Norma Complementar nº 11/2012 da Instrução Normativa nº 01 do Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR);

III. Devem ser avaliadas as instalações, os equipamentos e os processos, conforme as exigências previstas nas normativas institucionais e/ou governamentais vigentes;

IV. Os resultados das análises de conformidade devem ser divulgados à Diretoria Executiva da Fiocruz e às áreas de Tecnologia da Informação correlatas;

V. As análises de conformidade devem ser realizadas com periodicidade mínima anual.

Art. 31 – Comunicações

I. Cabe à COGETIC registrar, por meio da Central de Serviços, os problemas ocorridos no ambiente que possam impactar, de qualquer forma, os serviços das Unidades;

II. Cabe à COGETIC comunicar às Unidades, com antecedência mínima de 72 (setenta e duas) horas, as intervenções que possam causar indisponibilidade ou redução de desempenho dos serviços;

III. Cabe à COGETIC comunicar imediatamente às Unidades quaisquer eventos que impactem a disponibilidade ou o desempenho dos serviços.

Art. 32 – Continuidade de Negócios

I. Cabe ao Serviço de Segurança da Informação e Comunicações da COGETIC a gestão da continuidade de negócios da Sala Cofre da Fiocruz;

II. A elaboração dos planos de continuidade deve observar as diretrizes da Norma Complementar nº 06/2009 da Instrução Normativa nº 01 do DSIC/GSIPR, bem como o Modelo de Gestão de Continuidade de Negócios de TI da Fiocruz.

Art. 33 – Atualização de Sistemas de Gerenciamento de Conteúdo (CMS)

I. É responsabilidade da Unidade ou do desenvolvedor responsável pelo serviço manter o CMS atualizado com as versões oficiais. A não atualização poderá ser considerada risco à segurança institucional, conforme as diretrizes da COGETIC;

II. A COGETIC poderá, a seu critério técnico e sempre que identificado risco à segurança, aplicar atualizações forçadas com o objetivo de mitigar vulnerabilidades e preservar a integridade do ambiente da Nuvem Fiocruz;

III. Cabe à COGETIC a responsabilidade pela atualização dos Sistemas de Gerenciamento de Conteúdo, no que se refere à plataforma como serviço ofertada às Unidades, garantindo a correção de erros, atualização das versões do núcleo do CMS, compatibilidade com servidores e bancos de dados, bem como a infraestrutura dos servidores web, bancos de dados e sistemas operacionais, preservando a escalabilidade e disponibilidade das soluções, com o devido procedimento de backup.

SEÇÃO VI - DISPOSIÇÕES FINAIS

Art. 34 O Órgão Seccional (COGETIC) poderá alterar procedimentos técnicos dos serviços sem aviso prévio, desde que tais alterações não afetem o funcionamento dos serviços.

Art. 35 Cabe ao Órgão Seccional (COGETIC) convocar o Forum de TIC para discutir alterações em procedimentos técnicos que impactem o modo de operação das Unidades e/ou afetem diretamente o pleno funcionamento dos serviços.

Art. 36 Os serviços transversais, entendidos como aqueles comuns a toda a Fiocruz, serão mantidos exclusivamente pelo Órgão Seccional (COGETIC), não devendo ser replicados pelas Unidades Correlatas.

Art. 37 Os Órgãos Correlatos são responsáveis por todos os incidentes decorrentes da utilização dos serviços sob sua gestão.

Art. 38 Os Órgãos Correlatos têm ciência e concordam que seus dados, arquivos e informações armazenadas em suas contas e nas contas adicionais de usuários poderão ser apagados após o prazo de 60 (sessenta) dias corridos a partir da solicitação de cancelamento do serviço.

Art. 39 A Política de Uso da Nuvem Fiocruz, bem como o conjunto de documentos dela derivados, será

revisada e atualizada periodicamente ou sempre que necessário, respeitando o intervalo máximo de dois anos. A revisão será conduzida por Grupo de Trabalho composto por representantes das Unidades da Fiocruz e da COGETIC.

Art. 40 Para utilização dos serviços de hospedagem de sites e portais abrangidos por esta Política de Uso, a Unidade, por meio de seu Diretor ou Vice-Diretor de Gestão, deverá concordar e aceitar os termos e normas constantes da presente Política, mediante assinatura dos Anexos I - Termo de Hospedagem de Portais e II - Termo de Ciência e Responsabilidade, disponíveis nos modelos de documentos do Sistema Eletrônico de Informações – SEI.

3.0 - ANEXOS

ANEXO I - TERMO DE HOSPEDAGEM DE PORTAIS

I – INFORMAÇÕES DO SOLICITANTE			
Solicitante			
Local/Unidade		Data:	Tel. Fixo:
E-mail			Celular:
Nome do desenvolvedor			
Contato do desenvolvedor			

II – OBJETIVO DA HOSPEDAGEM			
Regras para definição do Nome do Site: Estar diretamente associado ao nome do projeto; Escolher um nome curto e fácil; Não são permitidos: acentos, cedilha, pontos e caracteres especiais.			
Nome			
URL			
Descrição			
Quais outros usuários terão acesso?			
Tempo de duração do Projeto?			
Tipo	□□□ Sistema WEB □□□ Site		
Possui banco de dados?	□□□ SQLServer □□□ MySQL □□□ PostgreSQL □□□ Não		
Quantidade de visitantes		Período Crítico de uso	
Linguagem de programação		Versão	
Impactos da indisponibilidade do serviço			
Relevância do serviço			

Criticidade Tempo Médio de Paralisação	

ANEXO II – TERMOS DE CIÊNCIA E RESPONSABILIDADE

Por este instrumento, declaro ter ciência e concordar com os termos expostos na Política de Uso do Centro de Dados para Computação em Nuvem, vigente no âmbito da Fundação Oswaldo Cruz – Fiocruz, consideradas suas normas e todas suas alterações, inclusive as deliberadas pelo grupo de trabalho, após a assinatura deste documento. Por esta razão, firmamos o presente para que produza seus devidos efeitos.

Rio de Janeiro, ____ de _____ de 2025

De Acordo,

_____

Nome:

Cargo:

Unidade:

Matrícula SIAPE:

ANEXO III - MATRIZ DE RESPONSABILIDADES

Descrição	Infra	Segurança da Informação	Cliente
Hospedagem	X		
Instalação, manutenção e atualização do SO	X		
Instalação dos serviços (WordPress, banco de dados, etc.)	X		
Atualização dos serviços (WordPress, banco de dados, etc.)	X		
Atualização dos serviços (WordPress, banco de dados, etc.)			X
Administração do WordPress			X
Manter recursos e aplicativos usados no site atualizados para evitar aumento da exposição às vulnerabilidades			X

Teste de invasão, análise de riscos ou análise de vulnerabilidades (de acordo com a criticidade do serviço)		X	
Emissão de certificado digital (quando aplicável)		X	
Monitoramento do serviço	X		
Gestão dos incidentes (receber, analisar, classificar e reportar)		X	
Buscar a implementação de ações de contenção/tratamento de um incidente de segurança			X
Execução do Backup do site	X		

4.0 - VIGÊNCIA

A presente portaria entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por **MISAEL SOUSA DE ARAUJO**, **Coordenador(ª) Geral de Gestão de Tecnologia da Informação e Comunicação**, em 11/09/2025, às 09:31, 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 http://sei.fiocruz.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5412179** e o código CRC **7E5F7235**.