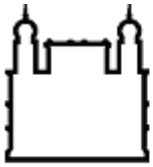

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Política de Uso do Centro de Dados para Computação em Nuvem da Fiocruz

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, exclusivamente, Plataforma como Serviço (*PaaS*) ou Software como Serviço (*SaaS*) às Unidades Correlatas da Fundação Oswaldo Cruz (Fiocruz). A Coordenação-Geral de Gestão de Tecnologia da Informação (COGETIC) será responsável em prover e manter o ambiente computacional e os beneficiados ficarão responsáveis pelo controle, administração, manutenção e atualização dos recursos que lhes serão disponibilizados.

Art. 2 O modelo de implementação adotado é definido sob a perspectivas de Nuvem Privada, isto é, infraestrutura de nuvem pertencente à Fiocruz e suas Unidades.

SEÇÃO II

DISPOSIÇÕES GERAIS

Art. 3 A presente política estabelece parâmetros para a administração do *Data Center* Fiocruz e uso do mesmo por suas Unidades.

Art. 4 A administração do *Data Center* é função específica da COGETIC/Fiocruz.

Art. 5 A administração e a atualização dos serviços ofertados serão da seguinte forma:

I. Serviços ofertados pela COGETIC e hospedados na nuvem Fiocruz é função da COGETIC/Fiocruz;

II. Os serviços que estão hospedados dentro do pool de recursos das unidades na Nuvem Fiocruz são de responsabilidade das unidades;

III. As unidades detentoras de um pool de recursos deverão manter atualizado o inventário dos respectivos servidores e serviços;

IV. A responsabilidade pela manutenção, atualização e funcionamento adequado dos serviços hospedados é exclusiva das Unidades (Plug-ins, Themas, Bibliotecas, Extensões e Dependências), que devem garantir que os sistemas, aplicações e conteúdos sob sua gestão estejam atualizados e em conformidade com as diretrizes institucionais. Corrigir falhas identificadas em tempo hábil, evitando impactos à disponibilidade e à segurança dos serviços. Solicitar suporte técnico à Cogetic apenas para questões relacionadas à infraestrutura de hospedagem, não incluindo intervenções nos sistemas ou conteúdos mantidos pela própria unidade. Monitorar periodicamente o desempenho e o uso dos serviços sob sua responsabilidade, adotando medidas preventivas quando necessário.

Art. 6 Para fins desta política, considera-se:

I. Data Center (Centro de Dados para Computação em Nuvem): local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma organização. Normalmente projetados para serem extremamente seguros, abrigam centenas de servidores, ativos de rede (switches, roteadores, etc) e bancos de armazenamento de dados (storages), processando grande quantidade de informação;

II. Sala Cofre: edificação física que comporta um Data Center. Deve fornecer mecanismos de segurança para permitir acesso somente a pessoas autorizadas, possuir câmeras de segurança, e sistema de combate e prevenção contra incêndios. O local deve ser refrigerado a fim de garantir que a temperatura do ambiente esteja em níveis aceitáveis para a operação dos sistemas, e principalmente, não apresente oscilações, que são extremamente prejudiciais ao funcionamento de qualquer equipamento. Deve garantir também que não haja falta de energia e tampouco oscilações em seu fornecimento que possam danificar equipamentos. Todos estes componentes citados devem ser redundantes e ativados automaticamente na falha do principal. A sala cofre deve contar com piso elevado para possibilitar a passagem de cabos elétricos e de dados, racks para armazenar servidores, storages, dentre outros, onde são montados os equipamentos e um ambiente totalmente controlado;

III. Órgão Seccional: termo utilizado para se referir à Coordenação-Geral de Gestão em Tecnologia da Informação - COGETIC, área Core do Centro de Dados para Computação em Nuvem;

IV. Órgão Correlato: termo utilizado para se referir às Unidades da Fiocruz - clientes do Centro de Dados para Computação em Nuvem;

V. Portal de Autosserviço: interface web para a interação com os serviços disponíveis na nuvem. Semelhante a uma “loja online”, é um portal acessível através de um navegador de internet (Chrome, Edge, Firefox), onde os recursos são disponibilizados aos usuários devidamente autorizados, e os recursos são gerenciados pelos Órgãos Correlatos;

VI. Templates de máquinas virtuais: máquinas virtuais padronizadas para cada tipo de serviço a ser implementado nela, Ex. Servidor web, servidor de Banco de Dados. Nele estará contido o mínimo de software necessário para o início da implementação do serviço. A instalação, gestão e atualização dos demais softwares ficarão a cargo dos Órgãos Correlatos;

VII. Central de Serviços – Sistema de requisições institucional que deverá ser utilizado para solicitar os serviços da Nuvem Fiocruz - https://centraldeservicos.fiocruz.br/.

Art. 7 Cada Órgão componente do SISP atua na operação, controle, supervisão e coordenação dos recursos de tecnologia da informação (TI) de sua esfera de atuação, compondo um sistema coordenado desde o nível central ao local, conforme mostrado na figura abaixo:

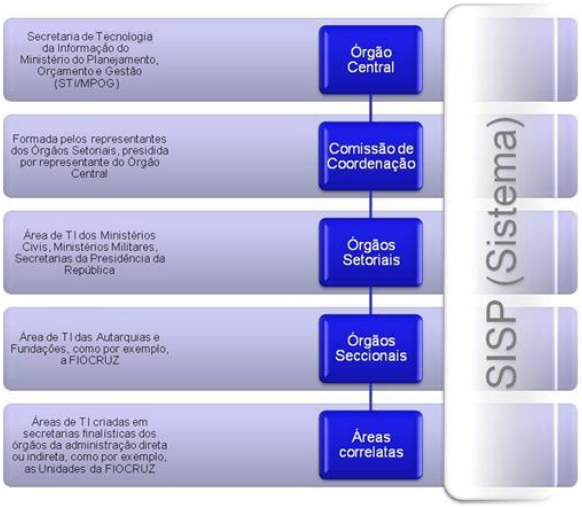

Figura - Estrutura do SISP, conforme Decreto nº 7.579 de 11 de outubro de 2011

SEÇÃO III

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

Art. 8 A Política de Uso do Centro de Dados para Computação em Nuvem tem por objetivo estabelecer parâmetros de gestão dos serviços da infraestrutura tecnológica Fiocruz, provendo a qualidade e estabilidade dos mesmos, bem como clarificar e regular as relações entre a COGETIC e as Unidades, atendendo aos seguintes princípios:

I. Reconhecimento do sistema SISP, conforme determinado pela Presidência da República no Decreto nº 7.579, de 11 de outubro de 2011, que estabelece ao Órgão Seccional, em seu art. 7º, inciso I, a responsabilidade de cumprir e fazer cumprir, por meio de políticas, diretrizes, normas e projetos seccionais, as políticas, diretrizes e normas emanadas do Órgão Setorial do SISP a que estão vinculados, e ao Órgão Correlato, neste mesmo decreto, em seu art. 8º, inciso I, subsidiar o Órgão Seccional no cumprimento de políticas, diretrizes e normas gerais relativas ao SISP;

II. Promoção da cooperação entre áreas e o empenho pela integração institucional, em conformidade com os valores institucionais da Fiocruz apresentados em sua Carta de Serviço ao Cidadão.

SEÇÃO IV

PADRÕES DE GESTÃO DE SERVIÇOS NO CENTRO DE DADOS PARA COMPUTAÇÃO EM NUVEM – DIREITOS E RESPONSABILIDADES

Art. 9 Os Serviços do Centro de Dados para Computação em Nuvem são gerenciados de maneira compartilhada, sendo parte desta gerência realizada pelo Órgão Seccional, e outra parte realizada pelos Órgãos Correlatos.

Art. 10 A COGETIC é a responsável pela manutenção da presente política, por receber eventuais contribuições das Unidades Fiocruz referidos a esta política e de garantir a coesão técnica deste documento.

Art. 11 O Comitê Gestor de TI, representado pela Câmara Técnica de Gestão da Fiocruz, é responsável pela avaliação e aprovação da presente política e de suas revisões anuais.

Art. 12 Atendimentos:

I. As solicitações de atendimento devem ser formalmente registradas na Central de Serviços;

II. Em caso de indisponibilidade da Central de Serviços, as Unidades poderão solicitar seus atendimentos diretamente com a Central de Serviços através do WhatsApp telefone (21) 97943-8777;

III. O catálogo de serviços e seus respectivos acordos de nível de serviço estão disponíveis na Central de Serviços;

IV. Após avaliação da elegibilidade do pleito, a solicitação será formalizada no SEI.

Art. 13 Serviço de *Backup*:

I. A COGETIC realizará cópias de segurança dos servidores virtuais de produção, cedidos para hospedagem de serviços das Unidades;

II. A unidade deverá informar quais serviços ou máquinas virtuais devem ser incluídos nas rotinas de cópias de segurança. Apenas backups de máquinas de produção serão realizados; máquinas de homologação e testes não serão incluídas nessas rotinas;

III. A COGETIC somente realizará cópias dos servidores virtuais, caso os serviços que estejam sendo executados nesses servidores, não sejam providos pela COGETIC. No caso de a COGETIC oferecer o serviço, este deverá ser migrado para as máquinas administradas pela COGETIC;

IV. A COGETIC deverá realizar operações de restauração dos servidores virtuais quando estes ficarem inacessíveis por causas físicas e/ou por problemas com ferramentas de virtualização. Os tempos para respostas às solicitações para início do atendimento, já estão definidos no catálogo de serviços da COGETIC. Iniciado o atendimento o tempo médio de recuperação é de 500 GB/h;

V. Toda solicitação de restauração deverá ser realizada através da Central de Serviços;

VI. Na ocasião de criação de novas máquinas ou serviços, a Unidade deverá informar a COGETIC para a inclusão na rotina de backup e de acordo com planejamento prévio;

VII. A COGETIC se exime de qualquer responsabilidade referente ao backup, caso a unidade não atenda às recomendações desta política.

Art. 14 Fica sob a responsabilidade do Órgão Seccional (COGETIC Infraestrutura Fiocruz):

Responsável por desempenhar o papel na resolução avançada de problemas técnicos aos servidores, oferecendo suporte especializado e contribuindo para a estabilidade e eficiência do datacenter, excetuando os servidores que estão em um pool de recursos administrados pelas unidades.

infraestrutura realiza a macrogestão do ambiente e tem as responsabilidades abaixo:

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, recomendações legais, recomendações dos órgãos de controle, e necessidades dos Órgãos Correlatos;

II. Disponibilizar acesso ao portal de "Autosserviço" aos Órgãos Correlatos que ainda tenham acesso direto a um pool de recursos, para que os mesmos possam gerenciar os recursos disponíveis para eles;

III. Criar, manter e fornecer o suporte necessário para a manutenção dos recursos cedidos para a hospedagem de serviços dos Órgãos Correlatos que ainda tenham acesso direto a um pool de recursos;

IV. Criar e atualizar regularmente os templates de máquinas virtuais a serem oferecidos no Portal de "Autosserviço", os quais virão apenas com o Sistema Operacional instalado em sua versão mais atual;

V. Avaliar a necessidade de criação de novos templates de servidores virtuais customizados que atendam às necessidades dos Órgãos Correlatos, caso os requisitos não estejam contemplados nos templates previamente oferecidos no Porta de "Autosserviço". Estes deverão estar de acordo com o tópico de Segurança da Informação contido na presente política de uso;

VI. Qualquer solicitação de suporte técnico deverá ser realizada através da Central de Serviços;

VII. Avaliar as solicitações recebidas dos Órgãos Correlatos através da Central de Serviços, referentes às operações no Centro de Dados para Computação em Nuvem, e atendê-las, caso a operação solicitada não represente risco à integridade dos serviços em questão, e estejam de acordo com todas as leis, jurisprudências, normas, regulamentos e políticas que regem o tema;

VIII. Informar aos Órgãos Correlatos com 3 (três) dias de antecedência sobre as interrupções necessárias para ajustes técnicos ou manutenções que demandem mais de 6 (seis) horas de duração e/ou que possam causar prejuízo à operacionalidade do serviço, salvo em casos de urgência, assim entendidos aqueles que coloquem em risco o regular funcionamento de nossa infraestrutura tecnológica.

Art. 15 Fica sob a responsabilidade dos Órgãos Correlatos (Unidades/Centros/Departamentos Fiocruz):

I. Administrar os recursos cedidos pelo Órgão Seccional, mantendo sempre o Sistema Operacional e demais aplicações com as últimas atualizações de versão e de segurança;

II. As licenças dos softwares dos templates das máquinas virtuais hospedadas no pool da unidade, bem como, Sistemas Operacionais, Banco de Dados, dentre outros, são de exclusiva responsabilidade dos Órgãos Correlatos. Não caberá ao Órgão Seccional (COGETIC Fiocruz) nenhuma responsabilidade pela compra de licenças, ativação, licenças piratas e nem o uso indevido delas;

III. É proibido a instalação de software pirata e identificado seu uso, a unidade correlata será notificada e a máquina virtual será excluída;

IV. O login e senha de administração do servidor serão criados pelo Órgão Seccional. Os Órgãos Correlatos deverão alterar a senha no primeiro logon;

V. A guarda do login e senha para acesso ao sistema é de exclusiva responsabilidade dos Órgãos Correlatos. Não caberá ao Órgão Seccional nenhuma responsabilidade pelo seu uso indevido;

VI. Órgão Seccional se exime de qualquer responsabilidade sobre a execução de backup caso o Órgão Correlato não atenda ao solicitado no inciso II do Art. 13 desta política;

VII. Solicitar, através da Central de Serviços, eventuais ajustes do pool de recursos que considerar necessários, ficando ciente que a solicitação passará por uma análise técnica da equipe da COGETIC;

VIII. Cabe à Unidade garantir um planejamento eficaz para a inclusão ou expansão de projetos que não ultrapasse o limite do pool de recursos disponibilizado;

IX. Respeitar todas as restrições e seguir todas as recomendações contidas na Política de Segurança da Informação e Comunicações – POSIC da Fiocruz vigente (Portaria nº 346/2012-PR). O descumprimento das ações de segurança contidas na POSIC e em suas normas complementares, será passível de sanções estabelecidas nesta política;

X. Implementar SSO (com MFA) em seus sistemas, a fim de evitar vazamento de credenciais em módulos de autenticação frágeis;

XI. Manter todas as aplicações devidamente atualizadas ou migradas para novos ambientes dentro do prazo estabelecido pela COGETIC e prévio à obsolescência dos recursos computacionais;

XII. Implementar, configurar, manter e monitorar soluções de segurança, mitigando ameaças e vulnerabilidades.

Art. 16 Fica sob responsabilidade de ambos os Órgãos (Órgão Seccional e Órgão Correlato):

I. Todo e qualquer sistema que envie e-mails, deve ser integrado ao serviço institucional de SMTP Seguro fornecido e mantido pela Cogetic;

II. Abster-se de fazer uso do serviço disponibilizado na Nuvem Fiocruz para propagar quaisquer tipos de mensagens de e-mail indesejadas (SPAM) a usuários ou grupos de usuários;

III. Esta restrição também se aplica a todo e qualquer envio de publicidade não solicitada (mala direta) via e-mail, como também o envio de qualquer tipo de e-mail não autorizado, de caráter geral, e/ou de qualquer outro tipo de mensagem eletrônica que motive reclamação de qualquer destinatário do mesmo e/ou de qualquer organismo e/ou indivíduo com funções de combate e repressão à prática de SPAM;

IV. Negligenciar-se da prática rotineira a fim de evitar qualquer ato do qual resulte o bloqueio do IP válido da Fiocruz por qualquer Órgão e/ou organismo ANTISPAM;

V. Abster-se de armazenar, nos recursos disponibilizados, conteúdo não relacionado à atividade fim da Fiocruz ou que de qualquer forma prejudique ou possa vir a prejudicar o funcionamento da Nuvem Fiocruz;

VI. Notificar qualquer incidente de segurança para a equipe de tratamento e resposta a incidentes da Fiocruz, via central de serviços.

SEÇÃO V

TRATATIVA DE DESCUMPRIMENTOS DAS REGRAS

Art. 17 O descumprimento de qualquer um dos termos da Política de Uso da Nuvem Fiocruz resultará em análise prévia para identificar se a causa da violação ocorreu intencionalmente.

Art. 18 Caso seja identificado que o descumprimento ocorreu de forma intencional, o autor estará sujeito a aplicação de medidas administrativas e legais cabíveis.

Art. 19 Correlacionam-se com a presente política, as Leis abaixo relacionadas, mas não se limitando às mesmas:

a. Lei Federal nº 8.159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

b. Federal nº 9.609, de 19 de fevereiro de 1998 (Dispõe sobre propriedade intelectual de programa 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 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências);

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. 20 Caso o descumprimento das regras implique em prejuízo à Fiocruz ou terceiros, de qualquer natureza, imediata ou iminente, os serviços poderão ser suspensos até que providências corretivas sejam tomadas pelo Órgão Correlato.

SEÇÃO VI
SEGURANÇA DA INFORMAÇÃO

Responsável por desempenhar o papel na proteção do ambiente, implementando medidas de segurança robustas para proteger ambiente de tecnologia, estabelecendo políticas de controle de acesso para garantir que apenas pessoal autorizado tenha acesso aos dados. Define as diretrizes gerais (POSIC) e implementa as ações de segurança para os ativos que estão no datacenter.

A Segurança da Informação realiza a macrogestão do ambiente e as orientações são encaminhadas para a administração geral da plataforma que devem implementá-las conforme necessidade, realizando abertura de chamado na Central de Serviços, quando necessário.

Art. 21 Fortalecimento (*hardening*):

I. O processo de *hardening* deverá ser conduzido sob a supervisão do Serviço de Segurança da Informação e Comunicações da COGETIC;

II. O Órgão deve realizar o *hardening* dos sistemas e serviços não disponibilizados pela COGETIC antes de colocá-los em produção;

III. O Órgão deve manter um processo contínuo de *hardening*, independentemente da origem do sistema operacional ou serviço;

IV. O Órgão deve revisar os protocolos de rede utilizados e desativar aqueles que não estejam em uso;

V. O Órgão deve utilizar as portas TCP/UDP default designadas a cada serviço;

VI. O Órgão deve revisar continuamente os serviços, aplicativos e pacotes existentes e desativar aqueles que não são necessários;

VII. O Órgão deve revisar continuamente contas e grupos de usuários, removendo aqueles que não estejam em uso;

VIII. Cabe à COGETIC aplicar as boas práticas de configuração a outros dispositivos, não limitando somente a sistemas operacionais ou serviços, mas estendendo aos componentes de rede, tais como: switches, roteadores etc;

IX. O Órgão deve buscar a aplicação de boas práticas de hardening disponíveis no mercado, encontradas no site dos fabricantes, listas reconhecidas de segurança, entre outros;

X. No caso de sistemas, serviços e aplicativos legados que não possam sofrer o processo de hardening, o Órgão deve garantir a implementação de controles que mantenham sua segurança em níveis adequados e instalação do Antivírus ou quaisquer outros softwares recomentados pela COGETIC;

XI. Sempre que possível, o Órgão deve usar ferramentas que verifiquem a base de pacotes, serviços e aplicações instaladas, correlacionando com informações de vulnerabilidades publicadas;

XII. As contas dos sistemas devem ter uma data de expiração definida;

XIII. A contas de usuários e grupos de sistemas devem utilizar o princípio do privilégio mínimo;

XIV. Deve ser adotada uma política de senhas com alto grau de complexidade combinada, sempre que possível, a outros fatores de autenticação;

XV. Deve ser instalado o agente do Workload Security.

Art. 22 Atualizações:

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 por ela mantidos;

III. A COGETIC deve disponibilizar repositórios para os sistemas operacionais ofertados como templates;

IV. Cabe à Unidade manter todos os recursos atualizados (sistema operacional, firmware, plug-in etc), independente da forma de atualização (versão, upgrade, patch, hotfix, etc);

V. A Unidade deve manter um ambiente de homologação, a fim de observar os possíveis impactos de uma atualização no ambiente de produção;

VI. As atualizações que possam impactar serviços transversais ofertados às Unidades devem ser comunicadas com o máximo de antecedência;

VII. A Unidade deve estabelecer um processo interno de implantação, testes e gerenciamento de atualizações;

VIII. A Unidade deve garantir a implementação de controles de segurança adequados para os sistemas, serviços e aplicativos legados que não possam sofrer processo de atualização;

IX. A Unidade deve adotar soluções para gestão do ciclo de vida de seus sistemas.

Art. 23 *Network Time Protocol* - NTP:

I. A Unidade deve sincronizar os dispositivos de rede com a hora legal brasileira através do serviço da Fiocruz;

II. O serviço NTP da Fiocruz é acessível através do servidor ntp.fiocruz.br.

Art. 24 Monitoramento:

I. Cabe à COGETIC monitorar toda a infraestrutura que compõe a Nuvem Fiocruz (Sala Cofre e Data Center) com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade;

II. Cabe à Unidade o monitoramento dos recursos e serviços alocados em seu Data Center Virtual;

III. O monitoramento deve possibilitar, minimamente, o envio de notificações aos responsáveis;

IV. O monitoramento deve ser utilizado de forma a não impactar o desempenho do ambiente.

Art. 25 Segmentação da rede:

I. A Unidade deve realizar estudo e planejamento quanto ao quantitativo de endereços IP's necessários à manutenção de seus serviços, submetendo-os formalmente e de forma antecipada à COGETIC para análise;

II. Cabe à COGETIC analisar o pedido de cessão de um novo bloco de endereçamento IP para a Unidade e avaliar a possibilidade de cessão.

Art. 26 *Firewall*:

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

II. A Unidade deve documentar as configurações do firewall virtual.

Art. 27 Gerência de vulnerabilidades:

I. Tanto a COGETIC quanto as Unidades devem implementar um processo de gerência das vulnerabilidades de seus serviços;

II. A Unidade deve realizar, periodicamente, análises de vulnerabilidades em seus sistemas e serviços;

III. Nos casos em que a Unidade não disponha de ferramentas para esta análise, o Serviço de Segurança da Informação e Comunicações da COGETIC poderá ofertar este serviço, através da abertura de solicitação, via Central de Serviços;

IV. A Unidade deve implementar, imediatamente, os controles necessários à correção das vulnerabilidades descobertas.

Art. 28 IDS/IPS *Malware*:

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

II. A COGETIC deve notificar à Unidade sobre comportamentos suspeitos em seu ambiente;

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

IV. Cabe à COGETIC implementar soluções de malware, IDS/IPS no ambiente virtualizado.

Art. 29 *Logs*:

I. A COGETIC mantém os 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. 30 Segurança de perímetro:

I. Cabe à COGETIC a gestão do Centro de Dados da Fiocruz, sendo este centro constituído por dois componentes:

a) Sala Cofre: ambiente seguro e certificado para operações de TI;

b) Data Center: conjunto de recursos para conectividade, processamento e armazenamento.

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

a) A gestão do ambiente da sala cofre;

b) Realização de análises de riscos dos aspectos operacionais, de negócio e estruturais do Centro de Dados, ao menos uma vez ao ano, cujos resultados devem ser divulgados à Câmara de Técnica Gestão e Desenvolvimento Institucional e às áreas de TI correlatas;

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

d) Administração dos contratos de manutenção do ambiente.

III. Cabe à COGETIC/Serviço de Infraestrutura Tecnológica:

a) A gestão dos recursos (equipamentos e serviços) do Data Center;

b) Administração dos contratos de manutenção do Data Center.

Art. 31 Gestão de incidentes de segurança da informação:

I. Os incidentes de segurança da informação serão tratados de acordo com o Modelo de Gestão de Incidentes de Segurança da Informação e Comunicações da Fiocruz.

Art. 32 Conformidade:

I. Cabe à COGETIC conduzir análises de conformidade do conjunto de recursos que compõem a "Nuvem Fiocruz", a fim de identificar a implementação de controles de segurança requeridos;

II. A análise de conformidade deve ser realizada ao menos uma vez ao ano, sendo pautada pelas diretrizes da Norma Complementar 11/2012 da Instrução Normativa 01 do DSIC/GSIPR;

III. Devem ser avaliadas instalações, equipamentos e processos, de acordo com exigências requeridas nas normativas existentes (institucionais e/ou governamentais);

IV. Os resultados observados nas análises devem ser divulgados à Câmara de Técnica Gestão e Desenvolvimento Institucional e às áreas de TI correlatas;

V. As análises de conformidade devem ser realizadas ao menos uma vez ao ano.

Art. 33 Comunicações:

I. Os problemas ocorridos no ambiente e que, porventura, possam impactar de alguma forma os serviços das unidades devem ser registrados pela COGETIC, através da Central de Serviços;

II. A COGETIC deve comunicar às Unidades, com 72 horas de antecedência, as intervenções que possam vir a causar indisponibilidade ou redução na performance dos serviços;

III. A COGETIC deve comunicar, imediatamente, às Unidades eventos que impactem a disponibilidade e a performance dos serviços.

Art. 34 Continuidade de Negócios:

I. Cabe ao Serviço de Segurança da Informação e Comunicações/COGETIC a gestão da continuidade de negócios da sala cofre Fiocruz;

II. A elaboração dos planos deve observar as diretrizes da Norma Complementar 06/2009 da Instrução Normativa 01 do DSIC/GSIPR e do Modelo de Gestão de Continuidade de Negócios de TI da Fiocruz.

SEÇÃO VII
DISPOSIÇÕES FINAIS

Art. 35 O Órgão Seccional pode alterar procedimentos técnicos dos serviços sem aviso prévio, desde que isso não afete seu funcionamento.

Art. 36 O Órgão Seccional é o responsável pela convocação do grupo de trabalho formado pelos representantes dos Órgãos Correlatos para discutirem alterações em procedimentos técnicos que alterem o modo de operação por parte dos Órgãos Correlatos e/ou afete diretamente o pleno funcionamento dos serviços.

Art. 37 Serviços transversais, ou seja, serviços comuns a toda Fiocruz, serão mantidos pelo Órgão Seccional, não devendo ser replicados pelas unidades Correlatas.

Art. 38 Os Órgãos Correlatos são responsáveis por todos os incidentes oriundos de sua utilização dos serviços.

Art. 39 Os Órgãos Correlatos têm ciência e concordam que seus dados, arquivos e informações armazenadas em sua conta e nas contas adicionais dos usuários poderão ser apagadas a partir de 60 dias corridos do pedido de cancelamento do serviço.

Art. 40 A Política de Uso da Nuvem Fiocruz, bem como, o conjunto de documentos gerados a partir dela, serão revisados e atualizados de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos, por um Grupo de Trabalho composto por representantes das Unidades Fiocruz e COGETIC. E posteriormente aprovado pelo Conselho Deliberativo da Fiocruz.

Art. 41 Para a utilização dos serviços expostos nesta política de uso, a Unidade, através de seu Diretor ou Vice-Diretor de Gestão, deverá concordar e aceitar os termos e normas constantes da mesma, mediante assinatura do Anexo I (Termo de Ciência e Responsabilidade).

Art. 42 Atualização de Sistemas de Gerenciamento de Conteúdo (CMS):

I. É responsabilidade da unidade ou do desenvolvedor manter o CMS atualizado com as versões oficiais;

II. A não atualização poderá ser considerada risco à segurança institucional;

III. 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.

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

ANEXO I

Termo 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 2024.

De Acordo,

_____

Nome:

Cargo:

Unidade:

Matrícula SIAPE:

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

ANEXO II

Termo de Hospedagem de Portais

Termo de
Hospedagem de Port