Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE SEGURANÇA FÍSICA EM DATA CENTER

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

APROVAÇÃO

APROVADA PELA PORTARIA 153/2013-PR

1. OBJETIVO

Este documento dispõe sobre as regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em Data Centers na Fiocruz.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Data Center: ambiente físico desenvolvido ou adaptado exclusivamente para hospedar os sistemas de informação ou equipamentos de TI.
Identificação física: crachá, credencial de acesso, etc.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ISO/IEC 73:2005 – Gestão de riscos – Vocabulário
- ISO/IEC 51:1999 – Safety aspects – Guidelines for their inclusion in standards

5. REGRAS

5.1. Disposições Gerais

5.1.1 O acesso ao Data Center é permitido aos agentes públicos credenciados e portadores da identificação física.

5.1.2 A identificação física dos agentes públicos lotados no Data Center deve ser distinta dos demais;

5.1.3 Os agentes públicos devem utilizar a identificação física em local de fácil visualização;

5.1.4 Os agentes públicos devem comunicar imediatamente a perda, furto ou desaparecimento da sua identificação física à área de segurança da informação;

5.1.5 A entrada de visitantes no Data Center só será permitida mediante autorização e acompanhamento por um agente público lotado nessa área, sendo obrigatório o registro do nome completo, RG, CPF, data e hora de entrada e saída.

5.2. Áreas de segurança do Data Center

5.2.1 Todas as instalações de processamento ou armazenamento de informações sensíveis devem ser mantidas em áreas de segurança do Data Center;

5.2.2 As permissões de acesso físico às áreas de segurança do Data Center devem ser mensalmente revisadas.

5.2.3 As áreas de segurança do Data Center devem ser claramente definidas com a utilização de barreiras de segurança e mecanismos de controle de acesso, de forma a impedir o acesso não autorizado;

5.2.4 Deve ser evitada a utilização de informações visuais que identifiquem as áreas de atividade de processamento e guarda das informações;

5.2.5 As portas das áreas de segurança do Data Center devem possuir mecanismos para fechamento automático.

5.3. Segurança ambiental

5.3.1 A localização do Data Center deve ser ocultada às pessoas que transitam em áreas públicas;

5.3.2 O Data Center deve estar situado, preferencialmente, em local de baixa frequência de desastres naturais ou causados por pessoas, e distante de áreas vizinhas perigosas;

5.3.3 O Data Center deve estar posicionado em local seguro, protegido por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso de acordo com criticidade associada aos seus ativos e informações;

5.3.4 As barreiras físicas a ser implementado para proteção do Data Center devem, caso necessário, ser estendidas da laje do piso até a laje superior, para prevenir acessos não autorizados ou contaminação ambiental, como as causadas por fogo ou inundação;

5.3.5 A edificação do Data Center deve ser protegida contra descargas elétricas atmosféricas;

5.3.6 A edificação do Data Center deve ser livre de sistemas de tubulação de drenagem pluvial, tubulação pressurizada de gases, exceto para a finalidade de combate a incêndio;

5.3.7 As portas e janelas do Data Center devem ser mantidas fechadas;

5.3.8 Todas as portas e janelas acessíveis ao público devem possuir sistemas de detecção de intrusos, periodicamente testados;

5.3.9 Áreas não ocupadas ou que possuam pouca movimentação de pessoal devem possuir sistemas de alarme de presença permanentemente ativo;

5.3.10 Os sistemas de alarme devem cobrir também as salas dos equipamentos de comunicação e voz;

5.3.11 Materiais combustíveis ou perigosos devem ser guardados de forma segura, a uma distancia apropriada das áreas de trabalho e áreas de segurança;

5.3.12 Suprimentos e materiais de escritório não devem ser armazenados em áreas de segurança, a menos que requeridos;

5.3.13 Equipamentos de contingência e mídias com cópias de segurança devem ser armazenados a uma distância segura da instalação principal;

5.3.14 Todo trabalho realizado por terceiros no Data Center deve ser registrado e supervisionado;

5.3.15 As instalações elétricas, de cabeamento lógico e dos equipamentos de detecção e combate a incêndio devem ser feitas de acordo com o especificado nas normas da ABNT;

5.3.16 É proibido o manuseio de alimentos, bebidas e cigarros, bem como o consumo no Data Center.

5.4. Instalação e proteção dos equipamentos

5.4.1 É proibida a ligação de mais de um equipamento em uma mesma tomada;

5.4.2 Os equipamentos de TI do Data Center devem ser instalados em *racks*, sempre que possível;

5.4.3 Todos os *racks* do Data Center devem ser seguros, possuírem portas dotadas de chaves em todos os seus lados e permitirem trancamentos, de maneira que as tomadas de energia permaneçam no seu interior e os fios e cabos sejam acondicionados sem contato com a parte externa, diretamente do piso para o interior do rack;

5.4.4 Os equipamentos cuja dimensão impeça a instalação dentro de racks devem ter seus botões de ligar/desligar devidamente protegidos contra acessos ou internamente desconectados, de forma a evitar seu acionamento local;

5.4.5 As chaves dos *racks* e dos quadros de força devem receber identificação e serem guardadas em um claviculário em local adequado, protegido contra acesso indevido;

5.4.6 Deve ser designado um responsável pela chave do claviculário, que deverá registrar todas as retiradas e devoluções de chaves;

5.4.7 A identificação adotada deve ser de difícil dedução para pessoas estranhas ao ambiente;

5.5. Segurança do cabeamento

5.5.1 Todos os cabos existentes no Data Center devem ser identificados;

5.5.2 Os pontos de rede excedentes devem ficar inativos;

5.5.3 O cabeamento deve ser implementado de acordo com a ABNT NBR 14.565:2007 - Cabeamento de telecomunicações para edifícios comerciais;

5.5.4 Os cabos de dados devem ser lançados em bandejas ou dutos rígidos, separados dos cabos e fios elétricos, de forma a evitar interferências eletromagnéticas;

5.5.5 Deve ser adotado piso elevado no Data Center de forma a facilitar futuras manutenções;

5.5.6 A estrutura do Data Center deve prover mecanismos de proteção, impermeáveis e à prova de fogo, em todas as suas dimensões, tais como, parede e piso, prevendo a passagem de cabos elétricos.

5.6. Sistema de combate a incêndio

5.6.1 Levar ao conhecimento da brigada de incêndio da Fiocruz a relevância do serviços contido no Data Center.

5.6.2 Realizar, em parceria com a brigada de incêndio da Fiocruz, ações de conscientização e capacitação dos agentes públicos quanto às ações a serem adotadas em situações de emergência, bem como montar e divulgar as rotas de fuga.

5.6.3 Instalar no Data Center, exceto sala cofre, extintores portáteis compatíveis com os tipos de materiais existentes (classe de fogo a ser combatido).

5.6.4 É proibido manter materiais inflamáveis (diesel, álcool, etc.) no Data Center.

5.6.5 É proibido o uso de chuveiros automáticos para extinção de incêndio (*Sprinkler*) no Data Center.

5.6.6 Devem ser instalados sistemas para detecção de fogo e fumaça como meio de alerta de incêndio.

5.6.7 Devem ser elaborados planos de teste dos detectores de fogo e fumaça, sendo executados mensalmente variando o local de procedência e a intensidade da fumaça.

5.6.8 Os detectores também devem monitorar a área abaixo do piso elevado e acima do rebaixamento do teto.

5.6.9 O sistema de alarme de incêndio deve possuir som distinto em tonalidade e altura dos demais dispositivos acústicos do Data Center.

5.6.10 Os equipamentos de combate a incêndio devem ser periodicamente inspecionados e testados por empresa tecnicamente qualificada, registrando-se a revisão.

5.6.11 Todos os agentes públicos que trabalham no Data Center devem ser capacitados para a utilização dos componentes do sistema de combate a incêndio, bem como saber interpretar os tipos de alarmes existentes.

5.6.12 Deve ser instalada uma rede de gás pressurizado, com tubos identificados e pontos de distribuição dimensionados especificamente para o Data Center, como meio de extinção de incêndio.

5.6.13 Os gases utilizados para extinção de incêndio devem ser inofensivos aos equipamentos, pessoas e meio ambiente.

5.7. Fornecimento de energia

5.7.1 Os circuitos específicos (elétrico, telefônico, sinalização, controle, sonorização e dados) devem ser identificados e instalados em eletrodutos ou bandejas separados dos demais circuitos de fornecimento de energia.

5.7.2 O circuito de energia que alimenta os recursos de tecnologia no interior do Data Center, deve ser estabilizado e separado dos demais circuitos.

5.7.3 Devem ser implementados estabilizadores centrais ou individuais equipados com filtros contra variação de tensão e com monitoramento por voltímetro.

5.7.4 As tomadas de energia localizadas no piso do Data Center devem possuir caixa protetora, garantindo seu fechamento quando não estiverem sendo utilizadas e evitando que objetos possam ser inseridos ocasionando curtos-circuitos.

5.7.5 Nobreaks e geradores de energia devem ser instalados, a fim de garantir a continuidade no fornecimento de energia aos equipamentos críticos para os serviços alocados no Data Center.

5.7.6 Os circuitos elétricos devem ser divididos e protegidos por disjuntores, dimensionados de acordo com normas específicas.

5.7.7 Os disjuntores dos quadros de distribuição de energia devem identificar claramente cada circuito elétrico.

5.7.8 O quadro de distribuição de energia, painéis de controle e caixas de passagem do cabeamento lógico devem ser protegidos contra acesso indevido.

5.7.9 Deve-se realizar mensalmente a verificação da voltagem e amperagem de energia de entrada no Data Center, mantendo-se o registro dos valores aferidos.

5.7.10 Somente circuitos de alimentação e controle relativos ao Data Center devem ser dispostos em seu interior.

5.7.11 A fonte de energia do sistema de controle de acesso deve ser contingenciado, evitando que, na ocorrência de falha, a entrada de pessoas não autorizadas seja permitida.

5.8. Controles de segurança do Data Center

5.8.1 Devem ser realizadas rondas de segurança em regime 24 X 7 no perímetro do Data Center.

5.8.2 Os acessos ao Data Center devem ser monitorados por circuito fechado de TV (CFTV). Câmeras de monitoramento devem ser instaladas em locais estratégicos do ambiente, seja ele interno ou externo.

5.8.3 Os circuitos das câmeras de monitoramento devem ser protegidos por conduítes de metal e ficar fora do alcance manual, evitando-se desativação intencional ou acidental.

5.8.4 As imagens captadas pelas câmeras do circuito interno de TV devem ser gravadas de forma contínua, visando embasar futuras investigações em caso de suspeitas ou incidentes de segurança.

5.8.5 Os arquivos das imagens gravadas devem ser guardados pelo período mínimo de um ano, sendo tratados com os mesmos critérios das mídias de cópia de segurança.

5.8.6 O sistema de circuito fechado de TV deve ser diariamente inspecionado, de forma a garantir a efetiva gravação das imagens.

5.8.7 As imagens gravadas pelo circuito interno de TV devem ser periodicamente analisadas, a fim de identificar possíveis eventos que contrariem a Política de Segurança.

5.8.8 O sistema de circuito fechado de TV deve ser monitorado, alertando a equipe em caso de indisponibilidade no funcionamento.

5.8.9 As portas de acesso ao Data Center devem possuir mecanismos de fechamento automático.

5.8.10 Alarmes de intrusão devem ser instalados nas portas e janelas do Data Center.

5.8.11 As portas de acesso devem possuir dispositivo de controle de acesso, tais como crachá por aproximação e solicitação de senha.

5.8.12 A entrada no Data Center deve ser condicionada a pessoas portando a identificação física (crachá) em local visível.

5.8.13 Após o horário normal de trabalho, o acesso para qualquer pessoa que não esteja envolvida na administração, gerenciamento ou operação do Data Center, será permitido somente através de autorização emitida pela chefia área de TI correlata.

5.8.14 É de responsabilidade dos agentes públicos lotados no Data Center, registrar e acompanhar os prestadores de serviço e visitantes, sendo responsáveis pelas ações destes enquanto permanecerem no ambiente.

5.8.15 A coleta de lixo e limpeza do Data Center deve ser realizada por pessoas instruídas quanto os cuidados necessários para tal serviço, devendo sempre ser autorizadas, registradas e acompanhadas por agente público lotado no ambiente.

5.8.16 Devem-se definir os dias e horários destinados à limpeza do Data Center, de forma a não comprometer a prestação dos serviços disponibilizados pela área.

5.8.17 A entrada e saída de qualquer ativo devem ser registradas.

5.8.18 É proibida a entrada de equipamentos de fotografia, vídeo e áudio.

5.8.19 É proibido comer, fumar ou beber no interior do Data Center.

5.8.20 Os ramais telefônicos devem ser restritos a chamadas internas.

5.8.21 Somente pessoas autorizadas podem portar equipamentos eletrônicos portáteis (celular, pen drive, palms, etc.) no interior do Data Center.

5.9. Sistema de ar condicionado

5.9.1 O sistema de ar-condicionado deve ser redundante.

5.9.2 O sistema de ar-condicionado deve ser, preferencialmente, do tipo *fan coil* e rede de dutos, utilizando caminhos redundantes e independentes entre si, através do teto rebaixo ou piso elevado.

5.9.3 Devem ser instalados filtros de limpeza no sistema de ar-condicionado para tratamento do ar circulante.

5.9.4 Os equipamentos externos de suprimento do ar-condicionado devem ser protegidos de ações ambientais ou humanas.

5.9.5 O fornecimento de energia elétrica do sistema de suprimento do ar-condicionado deve ser contínuo.

5.9.6 Os dutos de ar-condicionado devem ser revestidos por material térmico e não combustível.

5.9.7 O sistema de água do circuito de refrigeração deve ser protegido contra corrosão.

5.9.8 O termostato para controle de temperatura deve ser exclusivo para o Data Center.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.