



GOVERNO DO ESTADO DE SÃO PAULO  
SECRETARIA DA SAÚDE



INSTITUTO DE MEDICINA FÍSICA E REABILITAÇÃO  
do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo

# Política de Segurança da Informação Lógica



Rua Domingo de Soto, 100 Vila Mariana São Paulo – SP 04116-040



GOVERNO DO ESTADO DE SÃO PAULO



## Sumário

Introdução.....	4
Objetivo.....	4
Abrangência .....	5
Critérios Gerais.....	5
Sanções .....	7
Requisitos .....	7
Responsabilidades Específicas .....	8
Colaboradores em geral.....	8
Colaboradores temporários .....	9
Gestores .....	9
Custodiantes da Informação .....	9
Área de Tecnologia da Informação .....	9
Área de Segurança da Informação.....	11
Monitoramento e da Auditoria do Ambiente.....	11
Informação .....	12
Armazenamento de arquivos.....	12
Antivírus .....	13
Backup.....	14
Recuperação de Desastre .....	15
Identificação e controle .....	16
Usuário da rede.....	16
Nome do usuário.....	17
Senhas .....	17
Tempo de vida de contas e senhas .....	17
Controle de acesso lógico .....	18
Prazos de cadastramento de usuários .....	18
Impressão.....	18

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 2 de 30		



Email.....	19
Internet .....	22
Computadores e Recursos Tecnológicos .....	24
Ativos de tecnologia da informação .....	26
Empréstimo de equipamentos.....	27
Termo de responsabilidade .....	27
Softwares .....	27
Datacenter .....	27
Suporte Técnico da GeTI .....	29
Plantão à distância da GeTI.....	29
Considerações Finais.....	29
Referências.....	30

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 3 de 30		



## Introdução

A política de segurança da informação é o conjunto de diretrizes, normas e procedimentos que devem ser seguidos e visa conscientizar e orientar os colaboradores para o uso seguro do ambiente informatizado, com informações sobre como gerenciar, distribuir e proteger os principais ativos.

A política visa preservar confidencialidade, disponibilidade e integridade das informações e descreve a conduta adequada para seu manuseio, controle, proteção e descarte.

## Objetivo

Estabelecer diretrizes que permitam que todos os colaboradores do IMREA/HCFMUSP e da Rede de Reabilitação Lucy Montoro sigam padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal do Instituto e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações e o parque computacional da Rede de Reabilitação Lucy Montoro quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 4 de 30		



## Abrangência

Estas normas se aplicam a todos os colaboradores usuários dos equipamentos de TI, da rede de computadores e dos sistemas de informação em uso no IMREA/HCFMUSP e da Rede de Reabilitação Lucy Montoro.

## Crítérios Gerais

Esta política define os critérios para a segurança da informação, visando preservar a integridade, confidencialidade das informações da Rede de Reabilitação Lucy Montoro. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

Esta política é aplicável às informações da Rede de Reabilitação Lucy Montoro, que podem existir de muitas maneiras: escritas em papel, armazenada e transmitida por meios eletrônicos, exibida em filmes ou falada em conversas formais e informais. Seja qual for a forma apresentada ou o meio através do qual a informação seja apresentada ou compartilhada ela deverá estar sempre protegida adequadamente.

A política deve ser conhecida e obedecida por todos os colaboradores que utilizam os recursos de processamento da informação de propriedade da Rede de Reabilitação Lucy Montoro, sendo de responsabilidade de cada um o seu cumprimento. A política está disponível na intranet da Rede de Reabilitação Lucy Montoro (<http://intranet.redelucymontoro.org.br/Login.aspx>)

No âmbito da Rede de Reabilitação Lucy Montoro, somente é permitido aos colaboradores o uso de recursos de processamento da informação disponibilizados pela organização, de forma a garantir que os requisitos de segurança sejam atendidos.

Os Gerentes da Rede de Reabilitação Lucy Montoro são responsáveis em tomar as medidas cabíveis para o cancelamento do acesso aos recursos quando estes não forem mais necessários.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos colaboradores, quando na utilização dos recursos de processamento da informação da Rede de Reabilitação Lucy Montoro, ficando os transgressores sujeitos às sanções previstas pela lei.

Os documentos produzidos por intermédio dos recursos de processamento da informação da Rede de Reabilitação Lucy Montoro são de propriedade da Rede de Reabilitação Lucy Montoro. De igual modo, os programas desenvolvidos por colaboradores do quadro independente do seu tipo de vínculo.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 5 de 30		



As informações de propriedade da Rede de Reabilitação Lucy Montoro devem ser utilizadas apenas para os propósitos definidos no Regimento Interno da Organização. Os colaboradores não podem, em qualquer tempo ou sob qualquer propósito, apropiar-se dessas informações.

A identificação do colaborador, por meio de crachá, senha eletrônica ou outro meio, é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso o preenchimento de um termo de responsabilidade, indicando as suas condições de uso, seus direitos e deveres, que parte integrante do Manual do Usuário.

O cumprimento da Política de Segurança será auditado pelo Grupo de Segurança da Informação subordinado a GeTI - Gestão da Tecnologia da Informação. A Rede de Reabilitação Lucy Montoro se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso a Internet e o uso do Correio Eletrônico.

Os recursos de processamento da informação disponibilizados aos colaboradores tem que ser suportados por um projeto a fim de evitar situações de risco a segurança da informação. Antes de serem colocados em produção, terão que ser testados em ambiente de homologação.

Todas as informações devem ter classificação de segurança, aposta de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo

que, para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento. A classificação das informações deverá ser

realizada de acordo com norma específica de cada Gerência.

Todos OS colaboradores ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato, imediatamente, ao Grupo

de Segurança, através de e-mail ( [infraestrutura.geti.imrea@hc.fm.usp.br](mailto:infraestrutura.geti.imrea@hc.fm.usp.br) ).

O descumprimento das normas desta política implicará na aplicação de sanções administrativas, cíveis e penais cabíveis.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da GeTI – Gestão da Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos colaboradores como resultado de atividade profissional contratada pela Rede de Reabilitação Lucy Montoro, pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 6 de 30		



Os equipamentos de informática e comunicação, sistemas e informação são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Rede de Reabilitação Lucy Montoro, por meio da GeTI – Gestão da Tecnologia da Informação e a área responsável pela segurança Conectividade, Infraestrutura e Segurança, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

## Sanções

Com a identificação da violação destas normas, o usuário será notificado e as sanções aplicadas de acordo com a tabela abaixo:

Sanções	
<b>Primeira violação</b>	Será enviado email* de notificação ao usuário, informando qual a norma que foi descumprida.
<b>Segunda violação</b>	Será enviado email* de notificação ao usuário, com cópia para sua chefia imediata, informando qual a norma que foi descumprida.
<b>Terceira violação</b>	Será enviado email* de notificação ao usuário, com cópia para sua chefia e para o departamento de recursos humanos para tomada de medidas administrativas cabíveis de acordo com as normas da empresa.

\* No corpo do email será solicitado a confirmação via email do recebimento, no caso da não confirmação a notificação será enviada em papel.

## Requisitos

Para a uniformidade da informação, a Política de Segurança da Informação (PSI), deverá ser comunicada a todos os colaboradores da Rede de Reabilitação Lucy Montoro a fim de que a política seja cumprida dentro e fora da empresa.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 7 de 30		



Deverá constar em todos os contratos da Rede de Reabilitação Lucy Montoro, o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação e aos ativos computacionais, deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à GeTI na área de Conectividade Infraestrutura e Segurança.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo GeTI ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A Rede de Reabilitação Lucy Montoro exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta Política de Segurança da Informação (PSI) será implementada na Rede de Reabilitação Lucy Montoro por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

## Responsabilidades Específicas

### Colaboradores em geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 8 de 30		



Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Rede de Reabilitação Lucy Montoro e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

### Colaboradores temporários

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no termo de aceite concedido pela Rede de Reabilitação Lucy Montoro.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

### Gestores

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação da Rede de Reabilitação Lucy Montoro, por intermédio do Manual do usuário.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, que parte integrante do Manual do usuário assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Rede de Reabilitação Lucy Montoro.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta Política de Segurança da Informação.

### Custodiantes da Informação

#### Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política da Segurança da Informação.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 9 de 30		



só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para Rede de Reabilitação Lucy Montoro.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irreversível antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Rede de Reabilitação Lucy Montoro em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 10 de 30		



Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

### Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Rede de Reabilitação Lucy Montoro.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Rede de Reabilitação Lucy Montoro, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Buscar alinhamento com as diretrizes corporativas da instituição.

### Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta Política de Segurança da Informação, a Rede de Reabilitação Lucy Montoro poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 11 de 30		



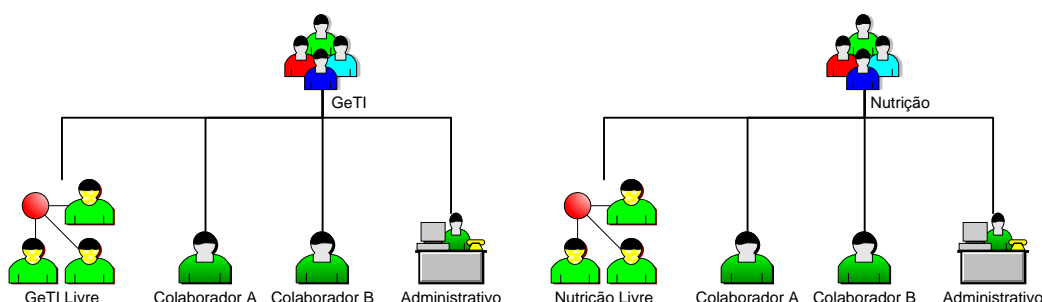
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior).
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

## Informação

As informações armazenadas na rede, seja em formato de arquivo, email, banco de dados, imagens, sons, e documentos, são de propriedade do Instituto de Reabilitação Lucy Montoro, e devem ser respeitadas quanto a seu acesso e divulgação. O acesso indevido, ou o uso de informações sigilosas podem ser motivo para sanções de acordo com normas da empresa ou legislação vigente.

## Armazenamento de arquivos

Nosso dispositivo de armazenamento de arquivos segue uma estrutura organizacional de acordo com ilustração abaixo, que representa parte desta estrutura (apenas os serviços GeTI e Nutrição):



Cada serviço do Instituto de Reabilitação Lucy Montoro tem uma pasta própria com seu nome. Nela está contido outras pastas:

- Uma pasta para cada usuário (colaborador) com acesso restrito.
- Uma pasta chamada “Administrativo” com acesso permitido a todos os membros do serviço.
- Uma pasta chamada “Serviço Livre” que tem acesso permitido a todos os usuários, independente a que serviço pertença.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 12 de 30		



Os arquivos gravados na rede estão protegidos pela cópia de segurança que é realizado diariamente.

**Arquivos gravados no computador (HD) não estão protegidos pela cópia de segurança**, e no caso de manutenção deste equipamento eles poderão ser apagados durante o processo de reinstalação do sistema operacional (Windows).

Podem-se gravar na rede quaisquer formatos de arquivo, desde que sejam comprovadamente para uso em trabalho. Não é permitido arquivos de música (mp3, wma, etc), de fotografia (jpg, jpeg, etc), de filmes (avi, mpeg, wmv, ogg, etc), caso seja necessário gravar estes formatos de arquivos deve-se solicitar a GeTI por escrito. Sem esta informação o arquivo poderá ser apagado pela equipe de Conectividade, Infraestrutura e Segurança da GeTI sem prévio aviso.

## Antivírus

O software antivírus utilizado na Rede de Reabilitação Lucy Montoro a partir 2014 será o Kaspersky Antivírus. Atualmente estamos utilizando o Avast Antivírus

O programa é composto por duas partes:

- Um agente de rede, que permite a instalação, manutenção e gerenciamento remoto do antivírus;
- O antivírus propriamente dito, que é responsável por manter o computador do usuário livre de ameaças eletrônicas.

A equipe de Conectividade, Infraestrutura e Segurança da GeTI da Rede de Reabilitação Lucy Montoro instala automaticamente esses programas nos computadores pelos quais ela é responsável (áreas administrativas e assistenciais). **Os usuários que forem responsáveis pela manutenção de seus próprios equipamentos deverão solicitar a instalação do antivírus à equipe de Conectividade, Infraestrutura e Segurança da GeTI da Rede de Reabilitação Lucy Montoro, através do e-mail: [infraestrutura.geti.imrea@hc.fm.usp.br](mailto:infraestrutura.geti.imrea@hc.fm.usp.br).**

Os equipamentos integrados nos domínios de rede da Rede de Reabilitação Lucy Montoro será instalado e gerenciado centralmente antivírus corporativos e automaticamente atualizado periodicamente.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 13 de 30		



## Backup

A política visa trazer uma solução de backup que realize o armazenamento das informações de forma segura e correta. Para esta política deverá ser avaliada a melhor solução de backup em fita com relação, a capacidade de armazenamento e rotina de backup para a Rede de Reabilitação Lucy Montoro, quando a solução for adquirida serão respeitadas as melhores práticas do fornecedor do equipamento.

As informações a serem armazenadas irão abranger os servidores de domínio, servidores de acesso remoto, servidor de arquivos ou volume disponibilizado em storage que estará armazenando os arquivos das unidades da capital, servidor de e-mail e base de dados do servidor Oracle Rack.

As informações serão armazenadas primeiramente em disco para que posteriormente em fita, assim trazendo a possibilidade de um restauro mais ágil. Dependendo criticidade do serviço será necessário à possibilidade de um restauro de forma granular, tendo como o exemplo “a possibilidade de restauro de uma mensagem de e-mail perdida”.

O backup em mídia removível poderá seguir o seguinte critério:

- De segunda-feira a sábado backup full;
- Aos domingos backup full;
- Último dia útil do mês backup full;

As cópias geradas no último dia útil de cada mês deverão ser enviadas para um local fora do Data Center, fornecer segurança e continuidade de negócio da Rede de Reabilitação Lucy Montoro.

A cópia de segurança das informações armazenadas no Datacenter será realizada diariamente pelo próprio Datacenter. Uma cópia em fita (Full) será entregue a GeTI mensalmente.

A cópia de segurança dos emails serão realizadas de acordo com a política de segurança do Datacenter, que proverá o serviço de email para a Rede de Reabilitação Lucy Montoro.

A logística da cópia de segurança deve permitir o restauro de arquivos históricos e informações num período de 1 dia a 1 ano.

Por questão de confidencialidade da informação, é terminantemente proibida a retirada e envio de cópia de segurança para qualquer local, não importando o motivo e nem a pessoa, ressalvo o motivo descrito acima.

O setor de infraestrutura faz parte da Gestão da Tecnologia e Informação, e é responsável pela realização e guarda da cópia de segurança.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 14 de 30		



## Recuperação de Desastre

Quando algum desastre ocorre, seja a inundação do Data Center, incêndio, explosões, terremoto, furacão, tsunamis ou qualquer outro tipo de desastre por causas naturais ou não, a primeira providência a ser tomada é a recuperação dos arquivos.

Para tal, o esquema de backup deverá estar religiosamente atualizado. Lembrando que as fitas, CD's Blu-Ray, HD's externos ou qualquer que seja a mídia no qual o backup dos arquivos são feitos, deverão estar sendo armazenados em lugar diferente do Data Center, de preferência em um cofre específico. Além do backup dos arquivos da rede, é muito importante ter uma imagem dos sistemas dos servidores.

A documentação técnica do Data Center (especificações técnicas da rede, configurações dos SO's, permissões e etc) também poderá te ajudar na recuperação pós desastre.

Em paralelo, a avaliação da infraestrutura deverá ser realizada, obter informações sobre o que está funcionando e o que realmente foi afetado servirá como base e previsão para a recuperação e disponibilização dos serviços de TI. Esta informação também servirá para a contabilização dos prejuízos e o custo para refazer a infraestrutura e equipamentos afetados.

A reconstrução de toda a infraestrutura e a substituição do hardware avariado dependerá de investimentos financeiros e tempo.

Nesta situação, é interessante reconstruir a infraestrutura já pensando em um próximo desastre de forma a evitar ou minimizar os danos, mesmo que isto se traduza em investimentos maiores. Estes investimentos se traduzirão em menos tempo indisponível e em menos dores de cabeça.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 15 de 30		



## Identificação e controle

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Instituição e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Instituição, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais, dados biométricos e cartões chaves têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Rede de Reabilitação Lucy Montoro e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O serviço de Recursos Humanos da Rede de Reabilitação Lucy Montoro é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

O GeTI responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários, acesso a sistemas.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

### Usuário da rede

O serviço de Recursos Humanos mantém atualizado o cadastro de funcionário no sistema Tasy. Só a partir deste cadastro é possível a criação de um usuário de rede e do sistema Tasy.

O colaborador retira no RH o Manual do usuário, que é uma síntese da Política de Segurança da Informação da Rede de Reabilitação Lucy Montoro e preenche o formulário de solicitação de

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 16 de 30		



senha, contido no manual e colhe a assinatura de autorização se sua chefia imediata. O formulário deve ser entregue na GeTI.

Neste formulário devem-se especificar os níveis de acesso permitido ao novo usuário. Após 2 dias úteis o usuário estará cadastrado e pronto para uso.

Na demissão ou afastamento do colaborador, o Recursos Humanos deve informar a GeTI para bloqueio da senha, do email, e dos arquivos.

### Nome do usuário

O nome dos usuários é composto pelo primeiro nome e último sobrenome, separados por um ponto. No caso de homônimo, o segundo sobrenome poderá substituir o último sobrenome.

Exemplo:

Nome do colaborador = Pedro Sousa Silva → Nome do usuário e email = pedro.silva

No caso de sobrenomes difíceis de pronunciar, ou que a combinação nome.sobrenome tornem o nome do usuário sujeito a ridicularidade, pode-se abrir ao colaborador a opção de escolha de seu nome de usuário.

### Senhas

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # \$ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 12 (doze) caracteres, alfanumérica, utilizando caracteres especiais (@ # \$ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

### Tempo de vida de contas e senhas

O usuário deverá ser forçado a trocar a senha no seu primeiro login.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a GeTI para liberação. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 17 de 30		



Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 60 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, o serviço de Recursos Humanos deverá imediatamente comunicar tal fato a GeTI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

### Controle de acesso lógico

Cada sistema utilizado pelos colaboradores tem controle de permissão de acesso. Os usuários que necessitarem utilizar qualquer um destes sistemas tem que apresentar solicitação da chefia imediata a GeTI (formulário de solicitação de senha).

### Prazos de cadastramento de usuários

Tabela de prazos de cadastramento de usuários e senhas

Usuário e senha	Quem cadastra	Prazo de cadastramento
Rede, email, Tasy	GeTI	2 dias úteis
SIGH	GeTI	2 dias úteis
BPA, Multimed, MV Faturamento e Scol	FFM	5 dias úteis
MV Suprimentos	HC	5 dias uteis

### Impressão

As impressoras devem ser utilizadas somente para trabalho e atividades profissionais. A GeTI monitora seu uso pelos colaboradores. Este monitoramento gera relatórios que são encaminhados a diretoria.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 18 de 30		



## Email

Cada email corporativo será vinculado a uma pessoa física, tornando-se responsável pela sua utilização.

O email será formado pela seguinte regra:

- Para colaboradores com vínculo CLT será formado pelo nome do usuário na rede (nome.sobrenome), acrescido de @hc.fm.usp.br, que deverá ser criado pelo próprio colaborador no site do Auto atendimento do HC.
- Para colaboradores sem vínculo CLT, ou seja, terceiros, pessoas jurídicas, menores aprendizes será formado pelo nome do usuário na rede (nome.sobrenome), acrescido de @redelucymontoro.org.br e será criado pela área de Conectividade, Infraestrutura e Segurança da GeTI.

Um colaborador poderá ter apenas um email corporativo.

Todos os colaboradores podem receber uma conta de email corporativa, desde que autorizados pela chefia imediata. O email corporativo deve ser utilizado apenas para comunicação de interesse da instituição, não sendo permitido spams, mensagens que possam infringir a legislação vigente, pirâmides, ou contendo fotografias pornográficas ou pedofilia.

Será utilizado como ferramenta padrão de acesso ao email o Webmail HC (Interface Gmail), que é uma ferramenta web.

Enquanto o colaborador estiver ativo na empresa seu email será privado, após seu desligamento o mesmo será bloqueado e permanecerá por 3 meses, podendo ser neste período reativado.

O objetivo desta norma é informar aos colaboradores quais são as atividades permitidas e proibidas quanto ao uso do email corporativo.

O uso do email da Rede de Reabilitação Lucy Montoro é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudicando e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 19 de 30		



INSTITUTO DE MEDICINA FÍSICA E REABILITAÇÃO  
do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Rede de Reabilitação Lucy Montoro ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Rede de Reabilitação Lucy Montoro estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Senac São Paulo;
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - vise obter acesso não autorizado a outro computador, servidor ou rede;
  - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - vise burlar qualquer sistema de segurança;
  - vise vigiar secretamente ou assediar outro usuário;
  - vise acessar informações confidenciais sem explícita autorização do proprietário;
  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - inclua imagens criptografadas ou de qualquer forma mascaradas;
  - contenha anexo(s) superior(es) a 20 MB para envio (interno e internet) e 20 MB para recebimento (internet)
  - tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 20 de 30		



INSTITUTO DE MEDICINA FÍSICA E REABILITAÇÃO  
do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo

- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Para colaboradores do IMREA e do Instituto de Reabilitação Lucy Montoro

Nome Completo (em negrito – identificação obrigatória)

Faculdade de Medicina da USP

IMREA HCFMUSP - Rede de Reabilitação Lucy Montoro

Serviço (em itálico – não utilize siglas) Ex.: Serviço de Fisioterapia; Comunicação Institucional; Finanças...

+55 (11) 0000.0000 ramal 000 / celular corporativo

[www.hc.fm.usp.br](http://www.hc.fm.usp.br)

[www.redelucymontoro.org.br](http://www.redelucymontoro.org.br)

*O emissor desta mensagem é responsável por seu conteúdo e endereçamento. Cabe ao destinatário cuidar quanto ao tratamento adequado. Sem a devida autorização, a divulgação, a reprodução, a distribuição ou qualquer outra ação em desconformidade com as normas internas da Rede de Reabilitação Lucy Montoro ou IMREA são proibidas e passíveis de sanção disciplinar, cível e criminal.*

*The sender of this message is responsible for its content and addressing. The receiver shall take proper care of it. Without due authorization, publication, reproduction, distribution or any other action not conforming to internal policies and procedures of Rede de Reabilitação Lucy Montoro or IMREA is forbidden and liable to disciplinary, civil or criminal sanctions.*

*El emisor de este mensaje es responsable por su contenido y direccionamiento. Cabe al destinatario darle el tratamiento adecuado. Sin la debida autorización, su divulgación, reproducción, distribución o cualquier otra acción no conforme a las normas internas del Rede de Reabilitação Lucy Montoro o IMREA están prohibidas y serán pasibles de sanción disciplinaria, civil y penal.*

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 21 de 30		

Rua Domingo de Soto, 100 Vila Mariana São Paulo – SP 04116-040

Tel.: 11-5180.7800 [www.reabilitahc.usp.br](http://www.reabilitahc.usp.br)



- Para diretores e chefes de serviço do IMREA e do Instituto de Reabilitação Lucy Montoro

Nome Completo (em negrito – identificação obrigatória)

Faculdade de Medicina da USP

IMREA HCFMUSP - Rede de Reabilitação Lucy Montoro

Cargo e Serviço (em itálico – não utilize siglas) Ex.: Diretora do Serviço de Terapia Ocupacional;

Coordenador de Controladoria e Finanças...

+55 (11) 0000.0000 ramal 000 / celular corporativo

[www.hc.fm.usp.br](http://www.hc.fm.usp.br)

[www.redelucymontoro.org.br](http://www.redelucymontoro.org.br)

*O emissor desta mensagem é responsável por seu conteúdo e endereçamento. Cabe ao destinatário cuidar quanto ao tratamento adequado. Sem a devida autorização, a divulgação, a reprodução, a distribuição ou qualquer outra ação em desconformidade com as normas internas da Rede de Reabilitação Lucy Montoro ou IMREA são proibidas e passíveis de sanção disciplinar, cível e criminal.*

*The sender of this message is responsible for its content and addressing. The receiver shall take proper care of it. Without due authorization, publication, reproduction, distribution or any other action not conforming to internal policies and procedures of Rede de Reabilitação Lucy Montoro or IMREA is forbidden and liable to disciplinary, civil or criminal sanctions.*

*El emisor de este mensaje es responsable por su contenido y direccionamiento. Cabe al destinatario darle el tratamiento adecuado. Sin la debida autorización, su divulgación, reproducción, distribución o cualquier otra acción no conforme a las normas internas del Rede de Reabilitação Lucy Montoro o IMREA están prohibidas y serán pasibles de sanción disciplinaria, civil y penal.*

## Internet

Todas as regras atuais da Rede de Reabilitação Lucy Montoro visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Rede de Reabilitação Lucy Montoro em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 22 de 30		



Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, email, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Rede de Reabilitação Lucy Montoro através do GeTI, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse da Instituição que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos referente as suas atividades.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Rede de Reabilitação Lucy Montoro para os meios de comunicação poderão manifestar-se, seja por email, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet não poderão fazer o download de nenhum programas. Se constatado a real necessidade e estiver ligados diretamente às suas atividades na Rede de Reabilitação Lucy Montoro e deverão procurar a GeTI.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo GeTI.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 23 de 30		



Os colaboradores não poderão em hipótese alguma utilizar os recursos da Instituição para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados a utilização de jogos.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Rede de Reabilitação Lucy Montoro ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da Instituição para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, Skype e afins) serão bloqueando e somente disponibilizados aos usuários que necessitem mediante a autorização de sua gerência.

O acesso a redes sociais (Facebook, Linked In, Twitter e afins) e sites de vídeos (Youtube e outros) não serão permitidos com exceção ao serviço de Comunicação Institucional que necessita destas ferramentas para desenvolver as atividades pertinentes ao trabalho.

## Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da Rede de Reabilitação Lucy Montoro, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 24 de 30		



GeTI, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente ao GeTI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o GeTI mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Instituição (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da Rede de Reabilitação Lucy Montoro e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do GeTI/Infraestrutura Conectividade e Segurança.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Os colaboradores devem informar ao GeTI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do GeTI ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pelo GeTI, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 25 de 30		



INSTITUTO DE MEDICINA FÍSICA E REABILITAÇÃO  
do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Instituição devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Situações em que é proibido o uso de computadores e recursos tecnológicos da Rede de Reabilitação Lucy Montoro.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

### Ativos de tecnologia da informação

No caso de mudanças física de equipamentos, somente a equipe da GeTI pode fazer a desinstalação e instalação. Solicite com no mínimo 2 dias de antecedência para agendamento.

Na compra de novos equipamentos de informática, a solicitação deve ser encaminhada a GeTI para pesquisa de mercado e cotação. Não é permitida a instalação ou remoção de software que não tenham sua licença em posse da GeTI.

Não é permitida a abertura dos equipamentos e seus periféricos para qualquer tipo de manutenção. Caso seja necessário qualquer tipo de reparo, este deverá ser solicitado a GeTI.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 26 de 30		



### Empréstimo de equipamentos

A GeTI detém a guarda de alguns equipamentos que são de uso comum, como notebook. Para solicitar estes equipamentos é necessário a solicitação por email para [suporte.geti.imrea@hc.fm.usp.br](mailto:suporte.geti.imrea@hc.fm.usp.br) e/ou agendamento pela agenda de eventos com 2 dias de antecedência. Caso o equipamento não esteja disponível o solicitante será avisado em tempo hábil.

### Termo de responsabilidade

Quando o usuário receber um equipamento de uso pessoal, em que for responsabilizado pela sua guarda e uso, deverá assinar um termo de responsabilidade, fornecido pela GeTI. Este termo é utilizado para notebook e qualquer outro dispositivo móvel, fornecido pela instituição para uso corporativo.

Sempre que possível será fornecido cadeado de segurança junto com o equipamento móvel.

### Softwares

A GeTI é responsável pela compra, instalação e configuração dos softwares utilizados, assim como a administração de suas licenças. O usuário que precisar de um software específico deverá solicitá-lo formalmente a GeTI, com justificativa da necessidade.

O usuário que trouxer algum software próprio para uso deverá entregá-lo a GeTI juntamente com a licença de uso, para homologação, aprovação e instalação pela equipe técnica.

### Uso de computador pessoal

Caso haja necessidade do uso de computadores pessoais dentro das dependências do Instituto, é necessário o registro deste dispositivo na GeTI. O computador será inspecionado e caso haja algum software que comprometa a segurança da rede, será solicitado sua desinstalação, caso não seja possível o equipamento será impedido de conectar-se a rede.

A senha de administrador do computador será alterado para uma senha de controle da GeTI durante o período de seu uso na instituição. Após este período a senha original será reintroduzida no computador.

O registro deste dispositivo terá validade por 6 meses, e deve ser atualizado após este período. O equipamento deverá ser entregue na GeTI, previamente agendado, e ficará para configuração durante 4 horas. Neste momento deverá ser entregue a senha de administrador do Windows.

### Datacenter

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão chave entre outros.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 27 de 30		



Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura conectividade e segurança, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede com acesso restrito.

Nas localidades em que não existam colaboradores da área de Gerencia de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Deverão existir cópias de chaves da porta do Datacenter com as pessoas responsáveis, uma das cópias ficará de posse do Gerente responsável pelo Datacenter, as outras, de posse da equipe de conectividade infraestrutura e segurança.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 28 de 30		



No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

## Suporte Técnico da GeTI

Toda manutenção e configuração dos equipamentos de TI devem obrigatoriamente ser realizado pela equipe técnica da GeTI.

As solicitações podem ser realizadas pessoalmente na GeTI de cada unidade, por email para o endereço [suporte.geti.imrea@hc.fm.usp.br](mailto:suporte.geti.imrea@hc.fm.usp.br), ou por telefone e os números estão disponível na intranet e no manual do usuário. Pelo telefone o usuário poderá ser orientado para solução do problema, quando possível. Por motivo de segurança, solicitação via email somente será aceita quando o remetente utilizar o email corporativo.

A GeTI mantém equipe de suporte técnico de segunda a sexta feira das 08 às 17 horas, fora deste horário os chamados serão recebidos no próximo dia útil. O telefone para suporte e abertura de chamados esta a disposição das 07 às 18 horas.

Fora do horário padrão de trabalho, e para casos emergenciais a GeTI mantém um suporte através do plantão a distância (via celular).

## Plantão à distância da GeTI

O plantão à distância da GeTI está à disposição dos usuários de segunda a sexta feira no horário noturno (das 18 às 07 horas), também aos sábados, domingos e feriados durante as 24 horas. O contato é através do celular número 11-99311-1920.

O intuito deste serviço é atender a chamados emergenciais. Estes chamados serão atendidos a distância, e quando for preciso a equipe poderá se deslocar para resolver o problema.

## Considerações Finais

Assim como Ética, Visão e Missão, a Política de Segurança da Informação deve ser entendida como parte fundamental da cultura interna de todos os colaboradores da Rede de Reabilitação Lucy Montoro, enfim, qualquer incidente de segurança subteme-se como alguém agindo contra a ética, visão e missão e os bons costumes regidos pela instituição.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 29 de 30		



## Referências

- **Política de Segurança da Informação** – Fundação Faculdade de Medicina, Departamento de Informática – julho de 2008, versão 7.
- **Política de Segurança da Informação Corporativa** – Hospital das Clínicas, Grupo de Segurança e Infra-estrutura Corporativa – maio de 2008.
- **Política de Segurança, Normas e Procedimentos da rede e dos sistemas do Instituto da Criança** – Divisão de Tecnologia da Informação em Saúde – janeiro de 2008.

VIGÊNCIA A PARTIR: 01/04/2014	APROVADO POR: Nome: Álvaro Zanetti Jr. Setor: Gestão da Tecnologia da Informação	DIRETORIA EXECUTIVA:
Página 30 de 30		