PSI – Política de Segurança da Informação 2018

Documento de Diretrizes e Normas Administrativas

V.4.0

HISTORICO DE REVISÕES

Data	Versão	Descrição	Autor
13/10/2016	1.0	Revisão PSI 2008	Grupo de segurança
15/09/2017	2.0	Revisão	Saulo Tadeu Correia
19/09/2017	3.0	Revisão ortográfica e políticas de backup, rpm, sysadmin, disp.móveis Inserido políticas de acesso ao Wifi.	Saulo Tadeu Correia
28/09/2017	4.0	Revisão geral	Saulo Tadeu Correia

Índice

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Fundação Faculdade de Medicina para a proteção dos ativos de ***informação*** *e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.*

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

A política está disponível na intranet http://intranet.ffmnet.br/Informatica/informatica.html, na seção Informática.

ESTRUTURA ORGANIZACIONAL

CONSELHO CURADOR

CONSELHO CONSULTIVO

DIRETORIA GERAL E VICE-DIRETORIA GERAL

SUPERINTENDÊNCIA SECRETÁRIA (CARGO VAGO)

SUPERINTENDÊNCIA FINANCEIRA

SUPERINTENDÊNCIA TÉCNICA (CARGO VAGO)

GERÊNCIAS

CONTROLADORIA

FINANCEIRO

FATURAMENTO E CONTROLE

SAÚDE SUPLEMENTAR

SAÚDE SUPLEMENTAR

MATERIAIS

RECURSOS HUMANOS

INFORMÁTICA

CONSULTORIA JURÍDICA

PROJETOS E PESQUISAS

OBJETIVOS

Estabelecer diretrizes que permitam aos usuários da Fundação Faculdade de Medicina seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa 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 seguindo as normas conforme:

- ***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.*
- ***Autenticidade*** *- propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo*
- ***Irretratabilidade*** *- propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.*
- ***Conformidade*** *- propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.*
- ***Custodiante do ativo da informação****: é aquele que de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.*

APLICAÇÕES DA PSI

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 conhecimento 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 Gerência de sua área sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela FFM pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações 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.

Esta Política é aplicável às informações da FFM, que podem existir de muitas maneiras: escrita 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 FFM, sendo de responsabilidade de cada um o seu cumprimento. A Política está disponível na intranet da FFM (http://portal.ffmnet.br/intranet). No âmbito da FFM, 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 FFM 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 FFM, ficando os transgressores sujeitos às sanções previstas pela lei.

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

As informações de propriedade da FFM devem ser utilizadas apenas para os propósitos definidos na Corporação. Os colaboradores não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

A identificação do colaborador, por meio de crachá, senha eletrônica ou outro meio, é pessoal 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.

O cumprimento da Política de Segurança será auditado pelo Grupo de Segurança da Informação subordinado ao Departamento de Informática.

A FFM se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à internet e o uso do Correio Eletrônico.

Os recursos de processamento da informação disponibilizados aos colaboradores têm que ser suportados por um projeto a fim de evitar situações de risco à 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 da Informação - FFM, através do e-mail (GrupoSeguranca@ffm.br).

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

SANÇÕES

Os técnicos e analistas da Informática identificarão os usuários que violarem qualquer item desta norma de segurança;

Na primeira violação, esses usuários serão notificados, via e-mail, do descumprimento das Normas estabelecidas neste documento; Caso haja uma segunda violação da Norma, esses usuários serão novamente notificados, via e-mail, sendo que uma cópia da notificação será enviada para o Gerente da área;

Na terceira violação, será encaminhada uma solicitação pelo gerente do departamento de informática ao departamento de recursos humanos para tomada de medidas administrativas cabíveis de acordo com as normas da empresa.

O funcionário poderá receber advertência administrativa, suspensão ou desligamento da empresa. Não é necessário que haja ***gradação*** *nas punições do colaborador, que poderá ser dispensado sem antes ter sido advertido ou suspenso, desde que a Diretoria entenda que a falta por ele cometida seja realmente grave.*

DAS RESPONSABILIDADES ESPECÍFICAS

1 – DOS 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.

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

1.2 – DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO (TI)

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.

***Gradação**: Aumento ou diminuição de maneira gradativa, continua de grau em grau, gradatividade.*

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

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 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, operacionais e educacionais 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.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a FFM.

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 irrecuperável 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.

***Custodiante**: pág. 7.*

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 empresa 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, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

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, podendo gerar históricos:

- *uso da capacidade instalada da rede e dos equipamentos;*
- *tempo de resposta no acesso à internet e aos sistemas críticos da FFM;*

- *períodos de indisponibilidade no acesso à internet e aos sistemas críticos da FFM;*

- *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);*

1.3 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, a Fundação Faculdade de Medicina 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;*

- *tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Grupo de Segurança da Informação;*

- *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.*

CORREIO ELETRÔNICO

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

O uso do correio eletrônico da FFM 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 prejudique a FFM e também não cause impacto no tráfego da rede.

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

- *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;*
- *enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a FFM 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 a FFM 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 da FFM;*
✓ *contenha ameaças eletrônicas, como: spam, mail bombing pág. 17, 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 explicita autorização do proprietário;*
✓ *vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;*
✓ *tenha conteúdo considerado impróprio, obsceno ou ilegal;*
✓ *seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;*
✓ *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;*

mail bombing: *Consiste em enviar milhares de mensagens idênticas para uma caixa de correio eletrônico para saturá-la.*

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

- *Nome do colaborador*
- *Gerência ou departamento*
- *Nome da empresa*
- *Telefone (s)*
- *Correio eletrônico*

Modelo de assinatura individual

Nome do Colaborador | Cargo
Área - FFM
Telefone: 55 11 xxxx-xxxx
Fax: 55 11 xxxx-xxxx
usuário@ffm.br

Modelo de assinatura por Grupo

Nome do Grupo | Informática
Área do Grupo - FFM
Telefone: 55 11 xxxx-xxxx
Fax: 55 11 xxxx-xxxx
grupo@ffm.br

INTERNET

Todas as regras atuais da Fundação Faculdade de Medicina 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 FFM, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos à internet

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, correio eletrônico, 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 FFM 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 de bom senso, desde que não cause impacto nas atividades corporativas.

Como é do interesse da FFM 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 de negócio.

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 poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na FFM.

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 pela Corporação.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da FFM 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 ao desenvolvimento 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 FFM 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 FFM 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 (Kazan, BitTorrent, Facebook, MSN, ICQ e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos

Não é permitido acesso a sites de proxy.

Os navegadores autorizados são respectivamente: Internet Explorer, Google Chrome, Mozilla Firefox e Opera fora estes navegadores como por exemplo Tor, Coowon, Torch, Lunascape, Ice Dragon, Vivaldi, SeaMonkey, Midori, Maxthon, Epic, Browzar e entre outros não serão aceitos no âmbito da FFM mesmo para fins de pesquisa.

OBSERVAÇÕES

Devido a bloqueio de sites com conteúdo inapropriados, alguns sites poderão ficar inacessíveis.

Caso seja bloqueado um site cujo conteúdo esteja de acordo com esta norma, o usuário pode solicitar o desbloqueio através do Sistema de Chamados, bastando informar na mensagem qual URL bloqueada;

O fato de um site não estar bloqueado não significa que o mesmo possa ser acessado pelos usuários.

Deverão ser observados todos os preceitos desta norma, desde a proibição de acesso a sites contrários a lei ao uso excessivo da internet para assuntos não relativos no horário do expediente por exemplo.

IDENTIFICAÇÃO

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 FFM 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 FFM, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos 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 FFM 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 Departamento de Recursos Humanos da FFM é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

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

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.

Recomenda-se por boas práticas que utilizem senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, exceto para sistemas limitados a 6, 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 recomenda-se que utilizem uma senha de no mínimo 10 (dez) 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.

Recomenda-se por boas práticas que as senhas não sejam anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não sejam 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 sejam constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário poderá ser bloqueada. No caso de desbloqueio é necessário que o usuário entre em contato com o suporte@ffm.br.
Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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 45 (quarenta e cinco) dias, não devendo ser repetidas as 8 (oito) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos podem exigir a troca de senhas a cada 30 dias. Os sistemas podem solicitar 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 Departamento ou o Supervisor da área deverá imediatamente comunicar tal fato ao Departamento de Suporte, 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.

DISTRIBUIÇÃO DE CONTAS E SENHAS

A conta de acesso à rede (login), de e-mail, permissão de acesso e acesso à sistemas devem ser formalmente solicitadas ao Suporte Técnico com antecedência mínima de 02 (dois) dias, através do formulário "Solicitação de Recursos de Informática", disponível no site da FFM.

DESLIGAMENTO DE CONTAS E SENHAS

A Gerência deverá comunicar às áreas responsáveis pela administração das contas o desligamento, afastamento ou remanejamento de qualquer usuário formalmente são solicitadas através de e-mail da Chefia direta do mesmo ou intranet pelo sistema de Help Desk da FFM.

Portanto, no desligamento de qualquer usuário os acessos serão imediatamente removidos impossibilitando o acesso aos recursos computacionais da organização, caso haja solicitação da gerência por meio do e-mail rede@ffm.br.

Para um novo usuário ou para aquele que esteja retornando após desligamento, afastamento ou remanejamento, a Gerência deverá solicitar a concessão de acesso mínimo necessário, para que este exerça sua respectiva tarefa.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do Fundação Faculdade de Medicina, 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.

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 departamento técnico responsável mediante registro de chamado no Sistema de Help Desk estabelecido pelo Departamento de Informática.

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 a FFM (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 FFM 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 da Gerência.

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

- *Os colaboradores devem informar ao departamento técnico 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 da área de (suporte FFM) 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 pela FFM, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade e informações que estão sobre a sua guarda.*

Ser protegidos por senha (bloqueados), nos termos previstos pela Identificação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

- *Todos os recursos tecnológicos disponibilizados pela FFM 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.*

- *Todos as estações deveram ter suas senhas de administrador (local) alteradas pelo suporte FFM, para que o usuário não tenha poder absoluto sobre a estação.*

- *Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da FFM.*

- *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 pais, a moral, os bons costumes e a ordem pública.*

ACESSO A VPN

O uso de um canal de Virtual Private Network(VPN) é permitido aos colaboradores da FFM explicitamente a área de TI ou terceiros desde que haja necessidade de acesso remoto para apoio ou suporte aos sistemas internos e com a autorização expressa do gestor do sistema ou Chefia imediata.

Sob o aspecto de proteção e integridade das informações, o acesso é classificado restrito ao colaborador ou prestador autorizado que devem estar cientes de suas responsabilidades de forma a garantir o cumprimento das normas descritas neste termo.

Colaboradores que têm atividades além do expediente normal ou por algum motivo não podem comparecer a FFM em caso excepcional também podem usufruir de um canal de VPN, mediante autorização expressa do responsável dos dados ou da Chefia imediata.

Todos os usuários de VPN possuem prazo limitado de uso, renováveis pelo mesmo período, desde que haja a anuência expressa da sua Chefia imediata.

Não compartilhar a chave privada e a credencial de acesso fornecida pela infraestrutura de redes da FFM.

Sempre manter atualizado softwares de antivírus e anti-spywares e estar com as últimas atualizações críticas e de segurança do Windows no equipamento cliente que realiza a conexão VPN.

A liberação do uso do acesso a VPN são feitas por meio de chamado e formulário.

UTILIZAÇÃO DE SOFTWARES PARA ACESSO REMOTO

- *A utilização deste software só deve ser permitida por colaboradores que prestam apoio ao usuário final, ou computadores específicos que necessitam de acompanhamento;*
- *A utilização do software só deve ser realizada com a permissão do usuário final;*
- *O login e senha de acesso é a mesma autenticação do login e senha da rede.*
- *O acesso remoto a computadores da FFM, deverá ser feito apenas mediante autorização da sua Chefia imediata.*

DISPOSITIVOS MÓVEIS

A Fundação Faculdade de Medicina disponibiliza o acesso móvel a seus colaboradores. Por isso, permite que eles usem equipamentos portáteis, sendo eles de uso particular ou corporativo.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Chefia direta, como: notebooks, smartphones, tablets e pen drives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A FFM, na qualidade de proprietária dos equipamentos fornecidos de uso corporativo, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na FFM, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel de uso corporativo. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade da FFM e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel ou uso corporativo.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos de uso corporativo, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico ou analista do departamento de informática.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados e de acordo com os critérios estabelecidos nesta política.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela FFM, notificar imediatamente seu gestor direto e a Gerência. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a FFM e/ou a terceiros.

É extremamente necessário o uso de antivírus em dispositivos móveis de uso particular ou quando disponibilizadas pela instituição ao colaborador ou utilizados por terceiros para se conectar nos âmbitos da FFM.

O colaborador pode usufruir quando disponível pela FFM de benefícios promocionais na aquisição de software de antivírus ou utilizar de um antivírus particular atualizado para proteção dos seus dados ao se conectar nos âmbitos da FFM.

DATACENTER

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

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 da equipe de infraestrutura, 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 ***Documento Central de Alarmes*** *disponibilizado pela infraestrutura de redes e salva no diretório de rede.*

Nas localidades em que não existam colaboradores da área 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 Documento Central de Alarmes, 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 no ***Documento Central de Alarmes****.*

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 que produza fumaça ou inflamável.

Não utilizar os pontos de energia (tomadas) conectados ao No-break responsável pela disponibilidade dos servidores.

Não utilizar os pontos de rede e telefone para conectar notebook ou qualquer outro dispositivo sem previa autorização do setor de redes

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 ***Documento de Movimentação de ativo imobilizado*** *disponibilizado na intranet.*

Manter a porta de acesso sempre fechada para não comprometer a climatização do ambiente.

No Datacenter que possui alarme, garantir que esteja acionado após deixar o ambiente.

A organização física dos dispositivos e servidores não dever ser alterada ou comprometida.

Em caso de irregularidades com o ambiente, notificar imediatamente o setor de infraestrutura..

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 nos termos do ***Documento Central de Alarmes****.*

BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida

(quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros definir responsabilidade do operador do backup em relação ao tempo de RTO e LTO pág.35.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter, diariamente são removidas da tape para o cofre e enviadas semanalmente para a guarda externa.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

Utiliza-se também para realização de Backup sistemas de cópia sombra nos servidores de arquivos e repositórios.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Documento de Limpeza dos Tapes de Backup.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento da empresa, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a ***Norma de Classificação da Informação pág.41****, seguindo assim as determinações fiscais e legais existentes no país.*

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Backup.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis a sua Chefia Imediata.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e restore.

RTO*: O período de tempo máximo desejado antes de uma falha ou desastre durante o qual as alterações feitas aos dados podem ser perdidos como processo de uma recuperação.*

LTO*: O período de tempo máximo desejado para trazer um ou mais aplicativos, juntamente com seus dados, a um estado corretamente operacional.*

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

POLÍTICA DE SEGURANÇA WIRELESS (REDE SEM FIO)

1. FINALIDADES E OBJETIVOS:

1.1. *Esta política tem a finalidade de estabelecer as regras e orientar as ações e procedimentos na utilização da rede sem fio, além de garantir a continuidade dos serviços nos âmbitos da FFM*

2. DIREITO DE USO:

2.1. *A utilização deste recurso está disponível para:*

- *Colaboradores que estão devidamente ativos e registrados na instituição;*
- *Auditores e funcionários terceiros;*

3. REQUISITOS NECESSÁRIOS:

3.1. *Devido à autenticação dos usuários na rede sem fio da FFM ser baseada na norma IEEE 802.1x, somente equipamentos cujo sistema operacional suportam esta norma poderão se conectar à rede:*

- *Ter equipamento de rede sem fio compatível com a norma IEEE 802.11a, IEEE 802.11b ou com a norma IEEE 802.11g e IEEE 802.11n;*
- *Navegador Internet;*
- *Sistemas operacionais Windows, Linux, Android ou Mac OS;*

4. COBERTURA:

4.1. *Atualmente os seguintes locais oferecerão suporte com qualidade a tecnologia sem fio (Wi-Fi):*

- *Todo o Edifício Cláudia;*
- *Edifício Natalie (apenas nas salas do âmbito FFM)*
- *Rh;*
- *Faturamento;*
- *Diretoria;*

5. ACESSO E FUNCIONAMENTO:

5.1. *Para terceiros como auditores e prestadores de serviços o acesso é liberado através de um número gerado pelo sistema de gerenciamento Wifi.*

5.2. *Para acesso a colaboradores a autenticação é realizada pelo login e senha do usuário na rede.*

6. UTILIZAÇÃO DA REDE SEM FIO:

6.1. *Os usuários deverão conhecer as normas de acesso (Rever política de internet na página 17) à rede sem fio e estar ciente das penalidades que poderão ocorrer caso haja violação das políticas de uso, prevista na PSI.*

6.2. *O login e senha são de total responsabilidade do usuário, não sendo permitido o compartilhamento de informações sobre a utilização do wireless às pessoas e computadores não cadastrados;*

6.3. *Não é permitido: (Rever política de internet na página 17)*

6.4. *Considera-se violação das regras o seguinte:*

- *Divulgar sua conta de usuário e sua senha de acesso para qualquer pessoa. Estas informações são de caráter pessoal e intransferível.*
- *Utilizar o serviço para fins ilícitos e proibidos.*

- *Utilizar o serviço para transmitir ou divulgar material ilícito, proibido ou difamatório que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório, injurioso ou calunioso.*
- *Acessar conteúdo pornográfico e jogos on-line.*
- *Utilizar o serviço para transmitir/divulgar material que incentive discriminação ou violência.*
- *Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual.*
- *Obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.*
- *Interferir ou interromper o serviço, as redes ou os servidores conectados ao serviço.*
- *Usar de falsa identidade ou utilizar dados de terceiros para obter acesso ao serviço.*
- *Tentar enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação.*
- *Utilizar o serviço para intimidar, assediar, difamar ou aborrecer qualquer pessoa.*
- *Utilizar serviço de proxy para burlar sites com acesso não autorizado.*
- *Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos.*
- *Utilizar o acesso à internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet.*
- *Acessar sites pornográficos ou quaisquer outros sites que seu conteúdo não seja informativo ou educacional.*
- *Violar ou tentar violar os sistemas de segurança.*

- *Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da FFM.*
- *Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional.*
- *Utilizar os recursos computacionais da FFM para ganho indevido.*
- *Utilizar os recursos computacionais da FFM para intimidar, assediar, difamar ou aborrecer qualquer pessoa.*
- *Consumir inutilmente os recursos computacionais da FFM de forma intencional.*
- *Desenvolver qualquer outra atividade que desobedeça às normas apresentadas acima.*

7. PENALIDADES:

7.1. *O usuário é responsável por qualquer atividade a partir de sua conta (login) e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação judicial e administrativa apresentada à instituição e que o envolva.*

7.2. *Em caso de descumprimento das regras, o usuário estará sujeita ao infrator as penalidades apresentadas a seguir:*

- *1º infração: imediata suspensão do acesso por 7 dias;*
- *2ª infração: suspensão do acesso por período de 30 dias;*
- *3ª infração: suspensão permanente do uso da rede sem fio.*

7.3. *Os registros de reincidência serão armazenados enquanto perdurar o vínculo do usuário para controle e tomada de decisão.*

7.4. *Caso alguma violação de regra seja identificada, através do sistema de monitoramento, o usuário será bloqueado e notificado pelo e-mail de contato.*

NORMA DE CLASSIFICAÇÃO DA INFORMAÇÃO

OBJETIVO

Definir as diretrizes relacionadas à classificação da informação na FFM.

ABRANGÊNCIA

Esta norma aplica-se aos usuários que estejam relacionados a criação, processamento, comunicação e armazenamento de informações, seja no ambiente informatizado seja no convencional.

DIRETRIZES

✓ *Todas as informações geradas por sistemas ou usuários deverão ser classificadas em relação ao seu grau de exposição, podendo ser:*

- *Informação pública: Informação classificada como pública pode ser distribuída sem restrição, inclusive exposta na internet;*

- *Informação interna: Informação classificada como de uso interno deve ser limitada ao público interno FFM;*

- *Informação restrita: Informação classificada como restrita deve ser limitada ao grupo de usuários envolvidos com o assunto;*

- *Informação confidencial: Informação classificada como confidencial deve ser limitada ao mínimo necessário de usuários;*

✓ *Toda informação gerada por sistemas ou usuários é considerada de uso interno por padrão;*

✓ *Toda a informação pode ser reclassificada de acordo com a necessidade do negócio ou conforme seu ciclo de vida;*

✓ *Informações classificadas como restrita ou confidencial deverão passar por um processo de eliminação qualificada;*

✓ *O processo de classificação da informação deve ser considerado tanto no formato eletrônico como no físico;*

✓ *Sistemas de proteção à informação poderão aplicar medidas restritivas visando garantir o grau de exposição das informações, conforme sua classificação.*

PAPÉIS E RESPONSABILIDADES

Colaboradores:

- *Preservar o grau de exposição da informação, conforme sua classificação;*
- *Informar seu gestor e a área de informática sempre que tomar ciência de que os cuidados necessários para a manipulação de uma informação classificada não estiverem sendo tomados;*

Gestor:

- *Classificar ou reclassificar as informações sob sua responsabilidade;*
- *Conscientizar os usuários quanto ao grau de exposição das informações.*

Área de Informática:

- *Administrar sistemas de proteção à informação.*

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da FFM. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

REFERÊNCIAS

NBR ISO 27002

http://www.sp.senac.br/normaseducacionais/psi_normas_educacionais.pdf

http://ri.bmfbovespa.com.br/fck_temp/26_107/file/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%2020160513.pdf

http://www.ibge.gov.br/home/disseminacao/eventos/missao/Politica_de_Seguranca_da_Informacao_e_Comunicacoes_2016.pdf

http://sistemas.fm.usp.br/autoatendimento/files/PSI_FMUSP_01_2016_V1.0.pdf

TERMO INDIVIDUAL DE RESPONSABILIDADE

TERMO INDIVIDUAL DE RESPONSABILIDADE

Pelo presente instrumento eu _____ matrícula/CPF nº_____, perante o Departamento de Tecnologia da Informação da FFM, na qualidade de usuário dos recursos de processamento da informação, declaro estar ciente e concordar com a política de Segurança da Informação composta por Critérios Gerais, Normas, Procedimentos e Instruções.

Declaro, também, estar ciente de que os acessos por mim realizado aos recursos providos pela instituição são automaticamente monitorados.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de segurança da Informação e que, a não observância desses preceitos, implicará na aplicação das sanções previstas neste documento.

São Paulo, de_____de _____.

_____

(Assinatura)

VIGENCIA A PARTIR	APROVAÇAO	DIRETOR GERAL
Publicação na Intranet.		

Declaro estar ciente e de acordo com as normas e sanções descritas no documento PSI- Politica de Segurança da Informação, versão 4.0 de 28/09/2017.

S. Paulo 20/08/18

Data e Local

Prof. Dr. Flavio Fava de Morais – Diretor Geral