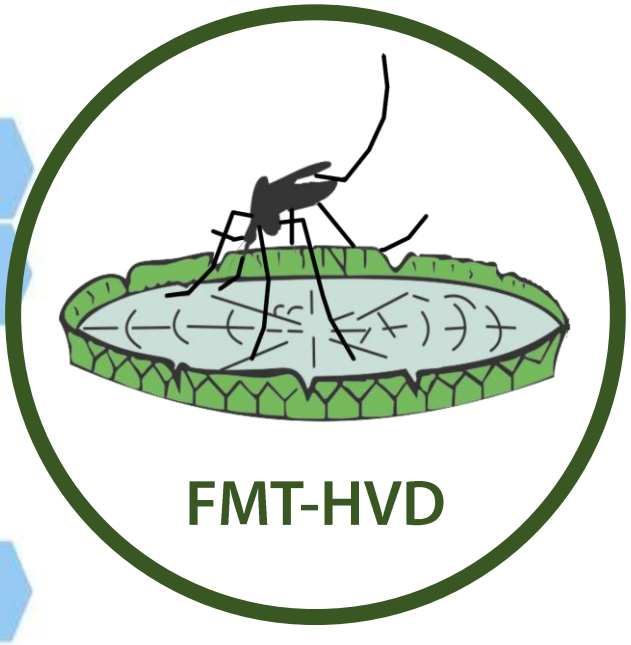
FUNDAÇÃO DE MEDICINA TROPICAL DR. HEITOR VIEIRA DOURADO

Política de Segurança da Informação

Versão 2



Manaus – AM
2024

Elaboração

Marcus Vinítius de Farias Guerra
Diretor Presidente

Flávio Azevedo de Lima
Diretor Administrativo e Financeiro

Moisés Leite Motta
Chefe do Departamento Técnico-Operacional

Clenilton Cruz de Alencar
Gerente de Informática

SUMÁRIO

1. Introdução

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas da FMT-HVD para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição. A PSI segue as leis vigentes no Brasil e foi elaborada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, NIST Cybersecurity Framework 2.0, CIS Critical Security Controls Version 8, reconhecidos mundialmente como um código de prática para a gestão da segurança da informação.

Esta PSI também é norteada pela Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD); Lei nº 10.695 de 02 de julho de 2003 (Lei Antipirataria); Lei nº 9.610 de 19 de fevereiro de 1998 (Lei de Direitos Autorais) e suas alterações, quando houver.

2. Conceitos e Definições

Ativo: todo e qualquer bem da FMT-HVD que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado essencial para a FMT-HVD, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição.

Bug Bounty: programa de recompensa por bugs que é oferecido por algumas organizações que recompensam os indivíduos por relatarem bugs.

Cavalo de Troia (Trojan horse): programa malicioso que cria abertura para outros programas e invasões indesejadas.

Código Executável: arquivo interpretado pelo computador como um comando de execução para determinadas funções.

Código Malicioso: programa que possibilita ações danosas, como vírus, *worms, trojans, spywares, malware, botnet, ransomware*, entre outros.

Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de contrato de trabalho com a FMT-HVD (Exemplos: funcionários e estagiários).

Colaborador Externo: qualquer pessoa contratada por empresa terceirizada que execute alguma atividade profissional nas dependências da FMT-HVD, sem vínculo empregatício (Exemplos: consultores e prestadores de serviços).

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Comunicadores Instantâneos: aplicativos que permitem interatividade, troca de conversas e conteúdos em tempo real. Ex. WhatsApp, Telegram, outros.

Custodiante: quem detém a guarda da informação, mas não é necessariamente seu proprietário.

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa por meio de recursos tecnológicos, como publicações na internet e o envio de fotos e vídeos com mensagens ofensivas pelo celular ou qualquer outro dispositivo móvel.

Dados Pessoais: informação relacionada a pessoa natural/física identificada ou identificável.

Dados Pessoais Sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: garantia de que os usuários autorizados obtenham, sempre que necessário, acesso à informação e aos ativos correspondentes.

Firewall: dispositivo que promove a proteção das redes contra invasões externas e acessos internos não autorizados.

Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.

Informação Sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para a FMT-HVD.

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com a FMT-HVD com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte.

Peer to Peer: arquitetura de redes de computadores em que cada um dos pontos funciona como cliente e servidor possibilitando o compartilhamento de arquivos. Habitualmente são utilizadas para o compartilhamento de vídeos e músicas.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Software de evasão de censura: programa que ignora a censura e políticas de segurança, permitindo que o usuário 'quebre' os filtros e condições de segurança impostos pelos firewalls.

Spam: e-mails não solicitados e normalmente enviados para um grande número de pessoas.

Usuário: todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pela FMT-HVD.

Vírus: programa malicioso que se propaga e infecta o computador.

Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

3. Objetivos da Política de Segurança da Informação

- Estabelecer diretrizes e normas que permitam aos funcionários, prestadores de serviços, estagiários e afins da FMT-HVD seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos;
- Nortear a definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
- Preservar a confidencialidade, a integridade e a disponibilidade das informações da FMT-HVD;
- Prevenir possíveis incidentes e responsabilidade legal da instituição e de seus funcionários, prestadores de serviços, estagiários e afins;
- Garantir a normalidade e a continuidade das atividades da FMT-HVD, protegendo os processos críticos contra falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e contratuais pertinentes à atividade da FMT-HVD;
- Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades da FMT-HVD resultante de uma falha de segurança;
- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;
- Garantir que todas as responsabilidades da Segurança da Informação sejam claramente definidas preservadas.

4. Aplicação da Política de Segurança da Informação

Todas as normas aqui estabelecidas devem ser aplicadas por toda a rede e seguidas por todos os funcionários, prestadores de serviços, estagiários e afins para a proteção da informação e para o uso racional de recursos tecnológicos.

Esta PSI compromete e responsabiliza cada usuário a manter-se atualizado sobre este documento e as normas relacionadas, buscando orientação da Gerência de Informática (GerInf) sempre que não estiver absolutamente seguro quanto ao acesso, aquisição e/ou ao descarte de informações e uso das estações de trabalho e demais periféricos.

Esta PSI também deve ser aplicada e respeitada, no que for oportuno, pelos alunos, acadêmicos, professores e preceptores.

5. Princípios da Política de Segurança da Informação

Os equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade.

Os alunos, estagiários e acadêmicos também devem usá-los para estudos, atividades educacionais e pesquisas acadêmicas.

Respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais é um preceito que deve ser seguido diariamente.

A FMT-HVD reserva-se o direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na instituição. Para tanto, são criados e implantados controles apropriados, mecanismos de monitoramento e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a FMT-HVD julgar necessário para reduzir os riscos, pautando-se na ética e na legalidade de forma a detalhar as ações em relatório específico.

6. Requisitos da Política de Segurança da Informação

A PSI deve ser comunicada a todos os funcionários, prestadores de serviços, estagiários e afins visando à efetividade e à real cultura de uso ético e legal dos recursos tecnológicos, bem como a Segurança da Informação.

Sempre que uma parceria ou contratação de empresa terceirizada envolver acesso a informações e/ou recursos tecnológicos da FMT-HVD, deverá haver comunicação expressa à Gerência de Informática.

A PSI e as Normas serão revisadas e atualizadas com periodicidade mínima de um ano ou sempre que houver um fato novo e relevante, conforme análise e decisão do Comitê Consultivo.

Todos os contratos da FMT-HVD devem constar o anexo ou a cláusula de confidencialidade para garantir o acesso aos ativos de informação. Mais informações, consulte a Norma de Uso de Ativos.

Já o uso de sistemas da FMT-HVD só é permitido para usuários que formalizarem a ciência sobre a PSI.

A responsabilidade em relação à Segurança da Informação deve ser atribuída ainda na fase de admissão do servidor/colaborador/terceirizado/aluno, de forma a ser incluída nos contratos e monitorada durante a sua vigência.

Para funcionários, prestadores de serviços, estagiários e afins, contratados em período anterior à publicação desta política, e que não tenham assinado os respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI para a respectiva assinatura de forma física (mesmo que coletivo) ou eletrônica.

Todos os funcionários, prestadores de serviços, estagiários e afins que tenham acesso a informações da FMT-HVD, devem passar por treinamento e conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela instituição. A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes.

Todos os requisitos de Segurança da Informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Serão criados e implementados também controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a FMT-HVD julgar necessário para reduzir os riscos aos ativos de informação.

Os ambientes de produção e de desenvolvimento tecnológico devem ser segregados e rigidamente controlados.

Um plano de contingência e continuidade tecnológico deverá ser implementado e testado anualmente integrado com plano de contingência e continuidade do negócio da instituição. O

objetivo é reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação.

Os ativos críticos ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados, além de ter o acesso controlado, registrado e monitorado. Para mais informações sobre ativos, consulte a Norma de Uso de Ativos.
Todo ativo de informação deve ser protegido de divulgação, modificação, furto ou roubo por meio da aplicação de controles.

Devem ser estabelecidas e comunicadas normas e responsabilidades pela propriedade e custódia dos ativos de informação. Bem como ser estabelecidos procedimentos e responsabilidades específicas para o uso e o gerenciamento dos ativos de informação oferecidos pela FMT-HVD, quando estiverem fora das instalações da instituição.

Todas as pessoas devem ser distintamente identificadas. Sejam visitantes, alunos, estagiários, parceiros, funcionários ou prestadores de serviços. Os dados coletados e armazenados devem ser segmentados a fim de que sejam aplicados controles especiais e sejam adequados às legislações pertinentes sobre a proteção de dados pessoais. Devem, ainda, ser estabelecidas regras para a coleta, o armazenamento e o tratamento de dados pessoais por meio de norma específica.

O uso de dispositivos móveis, assim como comunicadores instantâneos devem ser devidamente regrados em normativos próprios, atendendo sempre aos princípios da privacidade, respeito ao usuário e à necessidade da coleta de autorização, quando aplicável, devendo ser informado na Política de Privacidade, informações sobre as condições de tratamento.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação desta norma, ou ainda o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos de informação, o responsável e/ou solicitante deverá documentá-las imediatamente à GTI. Dessa forma será possível adotar medidas alternativas para minimizar riscos, bem como organizar um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

A FMT-HVD exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos aos usuários. Reservando-se o direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como

analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.

Esta atualização da PSI será implementada na FMT-HVD por meio de procedimentos específicos e obrigatórios a todos os funcionários, prestadores de serviços, estagiários e afins, independentemente do nível hierárquico ou função na instituição.
Todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente à GTI, que, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise. Toda e qualquer atividade que não estejam tratadas nesta política ou normativos específicos, devem ser realizados apenas após consulta e autorização do gestor da área.

O não cumprimento dos requisitos previstos nesta PSI e nas Normas de Segurança da Informação acarretará violação às regras internas da instituição, e o usuário estará sujeito a medidas administrativas e legais cabíveis.

7. Monitoramento e Auditoria

Para garantir as regras mencionadas nesta PSI, bem como para fins de segurança e prevenção à fraude, a FMT-HVD reserva-se o direito de:

- Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, internet, dispositivos móveis ou wireless, entre outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;
- Inspecionar qualquer arquivo que esteja em rede, no disco local da estação ou em qualquer outro ambiente para assegurar o rígido cumprimento desta PSI;
- Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;
- Instalar câmeras em suas dependências.

Os funcionários, prestadores de serviços, estagiários e afins tomam ciência de que ambientes, recursos tecnológicos, telefones, sistemas, computadores, dispositivos móveis e redes da instituição estão sujeitos a monitoramento e a gravação, atendendo à conformidade legal.

O uso de dispositivos móveis pessoais deverá ser objeto de norma própria, no entanto, o colaborador ou prestador de serviços tomam ciência, neste ato, de que ao aceitar ou optar pelo uso de dispositivos pessoais para fins corporativos, a FMT-HVD poderá auditar e inspecionar os recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos, sempre que considerar necessário, atentando-se à não discriminação e à proporcionalidade devida, respeitando a razoabilidade e privacidade.

8. Responsabilidades Específicas

8.1. Dos Usuários em geral

Funcionários, prestadores de serviços, estagiários e afins da FMT-HVD, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado à FMT-HVD e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

Cabe a todos os usuários as seguintes práticas:

- Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;
- Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;
- Assinar o Termo de Responsabilidade, formalizando a ciência da PSI e das Normas de Segurança da Informação, bem como assumindo a responsabilidade pelo seu cumprimento;
- Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pela FMT-HVD;
- Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da instituição;
- Prezar pela segurança das informações confidenciais, incluindo todo e quaisquer dados pessoais a que tiverem acesso;
- Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras da FMT-HVD.

- Comunicar imediatamente à GerInf sobre qualquer descumprimento ou violação da PSI e/ou de suas Normas e Procedimentos;
- Zelar pela integridade e confidencialidade de pastas e arquivos que sejam de uso comum do setor;
- Proceder a cópia de segurança dos arquivos sob sua responsabilidade, de forma integral e periódica;
- Manter sigilo sobre sua senha de acesso individual à rede de dados da FMT-HVD, não a compartilhando, mesmo que de forma eventual ou esporádica.

8.2. Política de Logins e Senhas

Os colaboradores, terceiros e passantes assumem inteiramente a responsabilidade pelo login (credencial) fornecido para acesso à rede, aplicações internas, externas (Cloud / SaaS), aplicativos móveis, internet e sistemas de forma individual e intrasferível.

A FMT-HVD sempre adotará, quando disponível pelo lado das aplicações, plataformas de validação de dois fatores (2FA/MFA) via aplicativo, e-mail, SMS ou outra forma. A verificação em duas etapas ajuda o uso das contas com mais segurança porque as senhas podem ser esquecidas, roubadas ou comprometidas. A verificação em duas etapas usa uma segunda etapa como seu telefone para dificultar a entrada de outras pessoas em sua conta. Recomendamos, sempre que possível e aplicável, o uso do aplicativo gratuito *Microsoft Authenticator*.

O uso de senha segura é obrigatório para os sistemas, serviços, dispositivos e devem ser configurados conforme o padrão definido pela FMT-HVD, sendo obrigatória a alteração da senha conforme periodicidade e recomendações de segurança determinada pela instituição.

Toda solicitação de credenciamento de novo usuário na rede deve ser formalmente direcionada à Diretoria Administrativa e Financeira. A solicitação deve conter os dados elementares do usuário (nome, CPF e – quando for o caso – prazo para desligamento da instituição), juntamente com a justificativa para acesso à internet, caso seja esse o objeto da solicitação. Essa solicitação formal não implica necessariamente deferimento automático.

O compartilhamento de logins de acesso é terminantemente proibido, podendo a Gerência de Informática proceder o bloqueio automático e sem prévio aviso caso haja verificado tal prática.

Da mesma forma, é prática não recomendada a anotação da senha de acesso em locais visíveis para uso comum.

É mandatório alterar a senha de acordo com a periodicidade definida pelo controlador de domínio ou administrador da rede, sempre que solicitado pelo sistema.

Caso o usuário esqueça sua senha, a geração de uma nova senha fica condicionada ao comparecimento do usuário à Gerência de Informática munido de documento de identificação pessoal / identidade funcional. Não será fornecida senha ou quaisquer informações sobre senha de acesso por telefone sob quaisquer hipóteses.

Caso a validade de uma conta individual tenha expirado, o chefe imediato deverá formalizar pedido para renovação da referida conta.

A depender do tipo de acesso e natureza do serviço, a Gerência de Informática poderá atrelar um login a determinada estação de trabalho, de modo que o referido usuário não poderá utilizar outro equipamento na rede.

Por razões de segurança, compliance e conformidade todos os usuários que utilizem dispositivos fornecidos e devidamente ingressados ao domínio da FMT-HVD, deverão fazer parte de grupos de usuários comuns, estando vetado o ingresso de usuários comuns ao grupo de administradores locais dos dispositivos.

As senhas, chaves de API (Keys), tokens não devem ser introduzidas, trafegadas pela rede, e-mail, aplicativos de mensagens instantâneas, anotadas e ou armazenadas em banco de dados, códigos fontes, linhas de comando, scripts, aplicações, sistemas web, APP ou API em texto simples, sendo necessário a utilização de criptografia forte e sempre aplicando o conceito de menor privilégio.

Recomendamos o uso de aplicativos específico para armazenamento de senhas que utilize criptografia forte e duplo fator de autenticação, sendo de responsabilidade do usuário buscar um recurso seguro e de boa reputação no mercado.

Fica vedado o acesso ao ambiente de servidores por terceiros sem o devido acompanhamento da Gerência de informática.

Para garantir um perímetro de segurança os acessos privilegiados, devem ser realizados por uma quantidade mínima de usuários, via cofre de senhas.

Para os casos extraordinários onde o gerente ou coordenador responsável da área assuma totalmente o risco, deverá ocorrer mediante assinatura do documento de Análise e Avaliação de Risco (AAR) e validação pela Gerência de Informática e Assessoria Jurídica da FMT-HVD.

8.3 Redes sem fio

Por padrão, o tipo de conexão promovida na rede interna da FMT-HVD é 'cabeada' (feita por meio de cabo de rede).

Não obstante, pontos de acesso foram disponibilizados como forma de suprir a carência de pontos de rede, configurando uma exceção à regra inicialmente descrita. Porém, a conexão fornecida por essas redes WiFi deve se limitar estritamente a atividades de consulta a páginas web, nunca para uso de sistemas de informação em produção.

Especialmente no que diz respeito ao acesso ao Sistema de Prontuário Eletrônico (Gestão Hospitalar), é vedado o uso de conexões WiFi, tampouco de conexões com dados móveis pessoais.

Os setores que contam com algum tipo de acesso WiFi ou rede própria sabeada, quer seja fornecido pela FMT-HVD quer seja via conexão independente (devidamente autorizada pela Diretoria), abdicam da conexão cabeada, estando vedado o uso simultâneo ou concomitante da rede cabeada da FMT com qualquer outra, ainda que não seja WiFi.

A Gerência de Informática não possui qualquer responsabilidade de manutenção ou controle de conexões independentes cuja instalação tenha sido autorizada pela alta direção da FMT-HVD.

8.4 Segmentação de ambiente, publicações internas e externas, estações de trabalho e e-mail institucional

Toda aplicação publicada (com origem no Datacenter da FMT-HVD ou não), bem como estações de trabalho que adentrarão a rede interna da FMT-HVD (ou dos recursos dela farão uso) deverão ser devidamente validadas pela Gerência de Informática.

8.4.1 Aplicações

As aplicações deverão ser classificadas como “de uso interno” ou “de uso externo” para adequação correta ao ambiente de publicação, considerando-se:
Internas: as aplicações que disponibilizam informações direcionadas aos colaboradores da FMT-HVD e que só possam ser acessadas a partir da rede lógica interna (intranet).
Externas: as aplicações que disponibilizam informações direcionadas para públicos externos e internos, e que podem ser acessadas a partir da internet, de forma pública/aberta ou mediante credenciais de usuário e senha.
Em todos os casos, as aplicações, suítes de aplicação, APIs e afins só poderão entrar em produção e efetivo uso no âmbito da rede de dados institucional depois de validadas pela Gerência de Informática, que avaliará, dentre outros aspectos:

- Se o uso da aplicação está alinhado às finalidades da FMT-HVD;
- Se a aplicação tem propósito geral;
- Se a aplicação é compatível com a arquitetura da rede ou das estações de trabalho;
- Se a aplicação possui requisitos mínimos de segurança e confiabilidade;
- Se a aplicação é de uso livre ou, se dependente de licença de uso, o setor demandante possui a referida licença de uso.

Para fins de exercício regular de direitos, atendimento de obrigação legal (Marco Cívil da Internet - Lei nº 12.965/2014) e legítimo Interesse, é necessário que as aplicações contenham registros de LOGS de criação de usuário, acesso a aplicação contendo as informações de identificação, registro de usuário, perfil, horário, ação e endereço IP (Público/Interno).

A Gerência de Informática se reserva ao direito de realizar testes que evidencie a segurança de uso da aplicação, tais como Análise de Vulnerabilidade e Teste de Penetração (Pentest), podendo vedar a instalação e uso da aplicação caso não haja preenchimento dos requisitos mínimos de segurança.

Fica a Gerência de Informática proibida de realizar a instalação de quaisquer aplicações, softwares ou sistemas proprietários dos quais não se possua a licença correspondente, a qual deverá ser apresentada no momento da solicitação formal do setor.

A instalação de softwares, aplicativos e sistemas externos em quaisquer das estações de trabalho da FMT-HVD que seja realizada por terceiros e que necessite de privilégios de administrador para sua realização deverá ser previamente agendada com a Gerência de Informática.

A Gerência de Informática pode, a qualquer momento e sem prévio aviso, realizar o bloqueio, inativação ou desinstalação (presencial ou remota) de quaisquer aplicações que seja identificada ou sabidamente nociva no âmbito da rede interna da FMT-HVD.

É vedado o uso de softwares de evasão de censura, como Ultrasurf, HotSpot, NordVPN, UrbanVPN, Freegate e qualquer outro da mesma natureza ou com mesma funcionalidade que venha a ser desenvolvido.

8.4.2 Estações de trabalho

Toda estação de trabalho que necessite adentrar a rede interna da FMT, ou que deseje utilizar os recursos dessa rede, deverá ser submetida à autorização prévia e ser configurada pela Gerência de Informática, que avaliará se a referida estação possui os requisitos mínimos de ingresso (sistema operacional e condições de uso). Uma vez configurada a estação de trabalho, fica o gestor do setor demandante correspondente ciente de que o acesso ao painel de controle e demais configurações do microcomputador ficará permanentemente bloqueado, sendo necessária a intervenção da Gerência de Informática sempre que houver real necessidade de ter as configurações do equipamento alteradas.

A Gerência de Informática poderá, a qualquer momento e sem prévio aviso, bloquear qualquer estação de trabalho caso seja verificado, por meio de análises de tráfego, que a referida estação está propagando conteúdo malicioso, ou disparando requisições de acesso contra as estações de trabalho internas da FMT-HVD ou com destino a servidores remotos (conhecidos ou não).

Toda estação de trabalho que possua acesso à rede corporativa da FMT-HVD é, necessariamente, patrimônio da entidade. Portanto, qualquer equipamento de cunho particular que venha ser empregado na rede corporativa para desenvolvimento de atividades cotidianas deve ser

incorporado ao patrimônio público por meio de termo de doação, pelo qual o proprietário original transfere a posse e a propriedade do equipamento à entidade.

É proibida a retirada dos equipamentos da FMT-HVD dos pontos de rede para conexão de dispositivos pessoais ou de terceiros.

Todo e qualquer remanejamento de equipamento, quer seja dentro do mesmo setor quer seja entre setores distintos, somente será feito pela Gerência de Informática mediante solicitação expressa do gestor do setor de origem.

Fica expressamente proibido:

- a mudança do local onde a estação de trabalho foi originalmente instalada;
- a utilização de roteadores, *switches* em cascata, HUBs, extensores ou quaisquer outros dispositivos que visem compartilhar uma conexão de rede para outros dispositivos simultaneamente;
- o uso de cabos de rede com comprimento maior que o fornecido pela Gerência de Informática;
- a conexão do microcomputador diretamente à rede elétrica;
- a remoção de quaisquer equipamentos de informática (dentro do setor ou para outro setor) sem a ciência do gestor setorial;

As estações de trabalho se destinam à realização das atividades setoriais alinhadas às finalidades institucionais da FMT-HVD. Jamais devem ser usadas para fins pessoais ou de entretenimento. De igual maneira, os arquivos mantidos nas referidas estações de trabalho devem manter estreita relação com as atividades-meio e atividades-fim de cada setor.

Por conta disso tudo, todo e qualquer arquivo ou pasta contido no computador jamais terá aspecto pessoal. Sua guarda deve ser garantida, inicialmente, pelo usuário que o criou e, secundariamente, pelo gestor setorial. Cópias de segurança regulares são de responsabilidade de cada usuário.

Assim, em eventual necessidade de realização de manutenção na estação de trabalho, que demande a formatação do equipamento (tarefa que elimina TODOS os arquivos do computador), fica cada usuário ou gestor setorial responsável pela guarda e segurança dos arquivos do setor. Fica isenta de responsabilidade a Gerência de Informática nos casos em que ‘arquivos pessoais’

tenham sido perdidos por eventual formatação de equipamento de usuário que não teve o cuidado de realizar a devida cópia de segurança, devendo reportar-se ao gestor setorial.

8.4.3 E-mail institucional

As contas de e-mail institucional devem ser utilizadas para as finalidades do setor, nunca para uso pessoal (ainda que seja uma conta individual).

Com o advento desta PSI, somente serão criadas novas contas institucionais setoriais.

O gestor do setor é o responsável por definir e guardar em segurança a senha de acesso à caixa de e-mail institucional. Da mesma forma, é o responsável pela guarda de todas as mensagens recebidas ou enviadas no âmbito do serviço público.

Fica o gestor setorial ciente de que, por eventual esquecimento da senha de acesso ou de quaisquer credenciais de recuperação, um chamado técnico será aberto junto ao órgão gestor do e-mail para a redefinição da senha. E que esse processo, sobre o qual a Gerência de Informática não possui ingerência, leva pelo menos 48h para conclusão.

8.5 Responsabilidades dos gerentes / gestores

Cabe a todo gestor de área:

- Garantir a implementação de mecanismos necessários para o descarte seguro das informações;
- Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os funcionários, prestadores de serviços, estagiários e afins sob a sua gestão;
- Cumprir e fazer cumprir esta política, as normas e os procedimentos de Segurança da Informação;
- Garantir acesso e conhecimento a esta política, bem como as normas e os procedimentos aqui estabelecidos;
- Inserir (quando possível) em contratos com prestadores de serviços, clientes, terceirizados e parceiros, quando estes necessitarem ter contato com informações da FMT-HVD, cláusula de responsabilidade, de Proteção de Dados Pessoais, de ciência da PSI e de confidencialidade, exigindo o repasse das obrigações a seus próprios empregados e colaboradores.

- Prezar pela conservação e integridade dos equipamentos de informática colocados sob sua responsabilidade, arcando com os prejuízos que eventualmente forem causados ao patrimônio público decorrentes do mau uso dos referidos equipamentos, inclusive com o ressarcimento ao erário;
- Garantir que as mensagens da caixa de e-mail institucional estejam íntegras e garantam a continuidade do serviço que delas dependerem;
- Garantir que os recursos tecnológicos oferecidos pela FMT-HVD sejam utilizados de forma racional;
- Comunicar à Gerência de Informática sobre o desligamento de funcionários, estagiários, terceirizados e demais colaboradores para os quais tenha solicitado acesso à rede ou a quaisquer sistemas de informação sob gerenciamento desta Gerência de Informática.

8.6 Responsabilidades dos Proprietários de Ativos de Informação

O proprietário da informação pode ser um gerente, coordenador e equipes de liderança de uma determinada área ou projeto, e será o responsável pela manutenção, revisão e cancelamento de autorização à determinada informação ou conjunto de informações pertencentes à FMT-HVD ou sob a sua guarda. Cabe ao proprietário da informação:

• Elaborar, para toda informação sob a sua responsabilidade, matriz que relaciona cargos e funções da FMT-HVD às autorizações de acesso concedidas;

• Manter registro e controle atualizados de todas as autorizações de acessos concedidas determinando, sempre que necessário, a pronta suspensão do acesso ou a alteração da autorização concedida;

• Reavaliar as autorizações de acesso, sempre que necessário ou solicitado, cancelando aquelas que não se fizerem mais necessárias;

• Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais;

• Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação prestando esclarecimentos quando solicitado.

• Todos os notebooks e dispositivos móveis que suportem o armazenamento de dados utilizados em trânsito deverão receber criptografia de disco.

9. Da Inovação e Uso de Novas Tecnologias

A FMT-HVD incentiva a inovação e desenvolvimento de novas tecnologias, para fins educacionais. No entanto, toda tecnologia a ser utilizada em nome da instituição ou como ferramenta de apoio na prestação de serviços, como sites, aplicativos, IoT, robótica, ambientes virtuais como o metaverso e Plataformas em Nuvem (SaaS) e o uso de Inteligência Artificial, deve ser homologada pela Gerência de Informática.

As tecnologias para atividade-meio são homologadas pela Diretoria Administrativa e Financeira e Departamento Técnico-Operacional. As tecnologias de uso transversal, para o processo de ensino e aprendizagem, são homologadas pela Diretoria de Ensino e Pesquisa. As tecnologias de uso específico das áreas de conhecimento, para o processo de ensino e aprendizagem, são homologadas pelas respectivas gerências. As tecnologias de uso na área de assistência serão homologadas pela Diretoria de Assistência Médica. Todos os processos de homologação são alinhados a parâmetros definidos pela Gerência de Informática.

Isso inclui análise prévia com base em riscos relacionados à Segurança da Informação e Proteção de Dados Pessoais, além dos riscos envolvidos na gestão do próprio negócio. Tais tecnologias quando aprovadas e homologadas passam a ser entendidas como uso institucional, devendo ser criado normas internas para sua utilização. A criação de perfis pessoais ou qualquer interação entre alunos e professores que não sejam por ferramentas ou assinaturas institucionais são de responsabilidade do próprio usuário, não possuindo, a FMT-HVD, qualquer gestão, ingerência ou responsabilidade por referidas ações ou qualquer ocorrência em tais ambientes.

Tecnologias inovadoras quando ainda em fase experimental e a utilização de equipamentos e ferramentas digitais, como sites, aplicativos, IoT, Robótica, ambientes virtuais como o metaverso e Plataformas em Nuvem (SaaS) e o uso de Inteligência Artificial, podem ser utilizadas apenas para fins educacionais, enquanto objeto de discussão e aprendizado e não como ferramenta institucional, não sendo permitido criação de contas pessoais para utilização em nome da FMT-HVD ou inserção de dados corporativos, bem como não será permitido a criação de contas corporativa/institucional sem que haja autorização do gestor e homologação pela Gerência de Informática.

10. Da Proteção de Dados Pessoais

A FMT-HVD em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados de forma permanente como dados confidenciais.

Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11º da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.

O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados em norma específica, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva norma.

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o “Privacy by Design / Privacidade desde a concepção”.

Além dos princípios mencionados, a FMT-HVD deverá elaborar um plano de resposta à violação de dados pessoais, elaborar o Relatório de Impacto sempre que necessário, utilizar processo de anonimização e pseudonimização sempre que possível/necessário, fazer registro das operações de tratamento de dados pessoais, utilizar protocolos de criptografia na transmissão e armazenamento de dados pessoais, bem como implementar um sistema de gestão de dados pessoais.

11. Das Disposições Finais

As infrações a esta PSI e às Normas de Segurança da Informação serão passíveis de processo disciplinar, podendo resultar de mera advertência até abertura de Procedimento Administrativo Disciplinar (PAD).

A qualquer tempo, e em qualquer um dos casos previstos, prevalecendo o descumprimento das regras expostas, a Gerência de Informática poderá bloquear temporariamente o acesso do usuário e comunicar os motivos à chefia imediata.

Não é permitido, dar suporte ou utilizar software, dispositivos, scripts, robôs ou quaisquer outros meios ou processos (incluindo *crawlers*, plugins e add-ons para navegadores ou quaisquer outras tecnologias) para fazer varredura no website ou copiar materiais e/ou quaisquer dados nele constantes. É vedada a realização de testes de vulnerabilidades dos mecanismos de segurança do website, app, aplicações ou da infraestrutura de tecnologia da informação utilizada em relação aos websites, assim como conduzir quaisquer pentestes no ambiente da FMT-HVD.

A FMT-HVD não possui nenhum programa de *Bug Bounty*, estando expressamente vedada a realização de atividades com tais fins.

O uso de qualquer recurso da FMT-HVD para atividades ilegais é motivo de responsabilização com possibilidade de abertura de Processo Administrativo Disciplinar, atuando a FMT-HVD na cooperação ativa com autoridades.

A PSI da FMT-HVD poderá ser complementada por Normas de Segurança da Informação que tratem assuntos relacionados ao uso de correio eletrônico, rede corporativa, internet, Proteção de Dados Pessoais, entre outros. E serão consideradas partes integrantes desta PSI.

Esta PSI estará disponível no website da instituição.

Normas específicas relacionadas a questões técnicas e confidenciais, e que requeiram acesso por equipes e pessoas específicas, devem ser colocadas à disposição apenas a pessoas autorizadas.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da FMT-HVD.