POLÍTICA INTERNA

SEGURANÇA DA INFORMAÇÃO

Versão 07/2022-2023

FUNEAS
Fundação Estatal de Atenção em Saúde do PR

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA SAÚDE

1 Sumário

2 SEGURANÇA DA INFORMAÇÃO EM AMBIENTES COLABORATIVOS – CONCIENTIZAÇÃO E COMPROMENTIMENTO

A Gestão da Segurança da Informação surgiu da necessidade de se minimizar os riscos ligados às informações gerais da organização.

Devemos nos preocupar com todas as formas de criação e tráfego de informação, seja ela em meio eletrônico ou em papéis. Assim, surgem as políticas e normas, com o objetivo de dirigir as empresas, evitando que outros funcionários ou terceiros, tenham acesso às informações digitadas e/ou escritas à mão, papéis deixados sobre a mesa ou em impressoras, assim como dispositivos móveis (CDs, DVDs, Pen Drives).

A Segurança da Informação é aplicável onde há informação: no armazenamento (Banco de Dados), no tráfego (Redes), no processamento e guarda, na impressão etc.

A Gestão da Segurança da Informação tem como foco principal as características humanas, organizacionais e estratégicas relativas à segurança da informação.

Nesta área, foram definidos os seguintes padrões e normas:

– Medidas para a Gestão da Informação

– Normas e Políticas; - Confidencialidade

– Mudança na Cultural Organizacional;

– Integridade - Conscientizar todos os envolvidos sobre a importância de boas práticas de Segurança da Informação;

– Disponibilidade – Envolver todos os funcionários e colaboradores, de tal modo que todos estejam comprometidos nessa prática;

3 OBJETIVO

Este documento estabelece as regras e os controles sobre o uso de recursos de tecnologia para preservar a integridade, confidencialidade e disponibilidade das informações do FUNEAS Fundação Estatal de Atenção em Saúde do Paraná.

4 APLICABILIDADE

Os dispositivos deste documento são aplicáveis a toda a FUNEAS e as 14 unidades geridas pela Fundação Estatal de Atenção em Saúde do Paraná, colaboradores, fornecedores e prestadores de serviços, que atuem nos ambientes físicos e/ou tecnológicos para processar dados sensíveis controlados e/ou pertencentes a FUNEAS.

5 RESPONSABILIDADES

5.1 Tecnologia da Informação

A área de Tecnologia da Informação é responsável por:

- Garantir a segurança da informação nos recursos utilizados pelos colaboradores;
- Analisar as contratações dos serviços de informática providenciando uma análise de custo/benefício;
- Validar e homologar todos os programas e equipamentos utilizados na FUNEAS e suas unidades geridas.
- Efetuar bloqueios de acesso a arquivos do domínio saude.parana, garantindo a qualidade e bom andamento dos trabalhos na FUNEAS;
- Avaliar a necessidade de aquisição de softwares, bem como a sua compatibilidade;
- Proceder à instalação dos softwares fornecidos pela CELEPAR (GSUS), Governo Federal e outros fornecedores.
- Prover suporte a todos colaboradores no tocante a infraestrutura operacional, equipamentos de informática que garantam aos mesmos o bom desenvolvimento das suas atividades;
- Manter a disponibilidade da infraestrutura e redes garantindo a sustentação da Equipe de Negócios;
- Direcionar fornecedores de Tecnologia a seguirem boas práticas de Segurança da Informação referente a Sistemas de Tecnologia implantados;
- Viabilizar e testar novas tecnologias que possam trazer melhorias para os sistemas e ferramentas utilizadas pelo colaborador;
- Acompanhar, juntamente com o usuário, o prestador de serviço, quando houver necessidades de atualizações de software/hardware, apresentações de novos aplicativos etc

5.2 Sistemas

A área de sistemas é responsável por:

- Suportar os sistemas utilizados pela Fundação Estatal de Atenção em Saúde do Paraná - FUNEAS.
- Aplicar as melhores práticas ITIL (*Information Technology Infrastruture Library*) no que tange, mudanças, incidentes, problemas e solicitações de sistemas;
  - Mudanças: Abrange alterações e implantações de sistemas cumprindo os requisitos ITIL que envolve aprovação e homologação dos usuários de negócios além de gerenciamento de risco e prioridades.
- Incidentes: Abertura de chamados para o mantenedor do código fonte a qualquer chamado dos usuários: *bugs,* mau funcionamento respeitando a SLA de cada fornecedor.
- Problemas: Quando um incidente se torna reicidente e é resolvido de forma paliativa é registrado o problema, juntamente com os fornecedores (caso aplicável).
- Solicitação/Demandas: Melhorias levantadas por colaboradores que são registradas para serem analisadas, debatidas e trabalhadas para serem implantadas.
- Analisar as contratações de novos sistemas providenciando uma análise de custo / benefício junto a diretoria as áreas.
- Os acessos restritos a sistemas, serão autorizados por e-mail apenas pela diretoria da Tecnologia da Informação.

5.3 Colaboradores

Os colaboradores são responsáveis por:

- Proteger seus acessos aos sistemas (login e senha), tratando-os de forma confidencial e exclusiva, sendo de sua inteira responsabilidade qualquer consequência da utilização indevida.
- Cuidar dos equipamentos sob custódia e desliga-los ao final do expediente;
- Respeitar regras de licenciamento de softwares.

6 DESCRIÇÃO DA NORMA

6.1 Considerações Gerais

A informação é um ativo essencial para os negócios da organização e consequentemente necessita ser adequadamente protegida. As diretrizes da Segurança da Informação visam preservar a integridade, confidencialidade e disponibilidade das informações da FUNEAS.

- Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas.
- Integridade: salvaguarda da exatidão e completude da informação e dos métodos de processamento;
- Disponilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Descrição de uma conduta adequada e segura para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais. Este Manual da Política é aplicável a todas as informações sob gestão da FUNEAS e unidades geridas, que podem existir de muitas maneiras: escrita em papel, armazenada e transmitida pelo correio ou por meio de meios eletrônicos, exibida em filmes ou falada em conversas formais ou informais. Seja qual for a forma apresentada ou o meio do qual a informação seja apresentada ou compartilhada, deverá estar sempre protegida adequadamente, de acordo com controles definidos neste Manual.

As informações de propriedade ou controladas pela FUNEAS devem ser utilizadas apenas para uso próprio de propósitos definidos. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações para uso próprio.

De acordo com a Política de Segurança da Informação da FUNEAS sempre que o usuário encontrar informações, aplicações ou procedimentos críticos sem o tratamento de segurança correto, deverá informar seu superior imediato para que sejam tomadas providências necessárias.

O não cumprimento das regras da Política de Segurança da Informação da FUNEAS, acarretará, no bloqueio do usuário nos computadores e sistemas até a averiguação pelo setor responsável.

6.2 Internet Corporativa

O serviço de Internet é disponibilizado exclusivamente para uso nas atividades profissionais.

O acesso às páginas da Internet, por meio dos recursos disponibilizados pela CELEPAR, caracteriza um instrumento de trabalho e, assim destina-se e limitasse à execução das

atividades pertinentes à função.

O acesso à Internet, por meio da rede corporativa, deve ser efetuado somente por equipamentos autorizados pela área de Tecnologia. A conexão à internet deve ser encerrada sempre que o usuário se ausentar de sua estação de trabalho ou ao término do uso da sessão.

O conteúdo é acessado através de login e senha expresso que libera o proxy, permitindo o acesso as páginas autorizadas pela Celepar. Além disso, o filtro de conteúdo impede o acesso a páginas indevidas de conteúdo malicioso, vírus e ameaças à segurança da informação, pois recebe atualização on-line sobre categorização de sites e conteúdo.

A Fundação Estatal de Atenção em Saúde do Estado do Paraná reserva-se o direito de examinar e de monitorar o acesso à Internet disponibilizada, em conformidade com os termos da Lei e de utilizar do conteúdo das trilhas de auditoria, sendo proibido:

- Utilizar os recursos da FUNEAS para fazer downloads (mp3, vídeos, programas diversos) de conteúdo que não seja para utilização no trabalho, distribuição de software de qualquer natureza e de dados não legalizados, bem como a distribuição destes;
- Acessar informações ilegais ou que possam ser consideradas ofensivas, intimidatórias, ameaçadoras ou similares, sendo que o usuário será responsabilizado pelos sites acessados e pelos arquivos copiados para a rede interna da Instituição;
- Acessar portais ou páginas com conteúdo de caráter obsceno, sexual, pornográfico, erótico, racista, constrangedor, difamatório, discriminatório ou preconceituoso (sexo, raça, etnia, religião, nacionalidade), ilegal, agressivo e abusivo ou de qualquer outra natureza, que atente contra a integridade moral e os bons costumes dos indivíduos ou de grupos da sociedade;
- Copiar programas freeware, shareware ou que não tenham sido adquiridos pelas formas legais e conformidade com as leis brasileiras e autorizado pela área de Tecnologia da Informação. A utilização de softwares não legalizados é considerada pirataria e pode causar danos aos cofres públicos e de imagem para o Governo do Estado do Paraná e a própria instituição FUNEAS.
- Utilizar softwares de troca de arquivos nos formatos *peer-to-peer* (P2P) ou torrent;
- Utilizar serviços de *streaming*, tais como rádios on-line e afins, a não ser que o acesso seja inerente a trabalhos, pesquisas ou negócios fa FUNEAS;
- Utilizar softwares de comunicação instantânea não homologados pela Tecnologia da Informação e previamente autorizados;
- Acessar e propagar qualquer tipo de conteúdo malicioso, como vírus, worms, cavalos de tróia ou programas de controle de outros computadores, bem como spam;
- Utilizar para jogos on-line, fóruns não profissionais, gincanas e concursos on-line;
- Utilizar a rede para fins comerciais, ilegais ou imorais;
- Utilizar para tentativa de ataque ou intrusão a outros computadores da rede interna ou externa;

- Utilizar para cópia, distribuição ou armazenamento não autorizado de material ou software protegido por leis de direito autoral, por qualquer meio;
- Disponibilizar a outro usuário sua conta de acesso, devendo seu login e sua senha ser tratados de forma particular, confidencial e exclusiva.

Caso a área de Tecnologia julgue necessário, poderá efetuar bloqueios de acesso a arquivos, domínios e serviços de Internet que comprometam o uso de banda, a segurança dos dados FUNEAS ou o bom andamento dos trabalhos. Com base em relatórios para análise de segurança dos sites acessados pelos colaboradores poderá haver restrição a determinados conteúdos/sites sem aviso prévio.

A Sede Administrativa disponibiliza uma rede wireless sem restrições de acesso para uso de equipamentos pessoais, esta rede é fisicamente apartada da rede corporativa, não sendo possível acessar com os equipamentos fornecido pelo FUNEAS, sem devidas autorizações pela área de Tecnologia da Informação.

6.3 Correio Eletrônico

O Correio Eletrônico é uma ferramenta essencial ao dia a dia, permitindo agilidade na comunicação interna e externa. As mensagens e os documentos eletrônicos estão sujeitos às mesmas leis e normas aplicadas a documentos escritos. O uso não controlado ou inapropriado desta ferramenta pode trazer ameaças reais, tais como:

- Criminal;
- Autoridades Regulatórias;
- Contaminação por Vírus;
- Quebra da Confidencialidade;
- Danos a Imagem.

Assim, como qualquer recurso provido pela FUNEAS, o uso dos serviços do correio eletrônico deve ser dedicado às atividades de interesse da Fundação Estatal de Atenção em Saúde do Paraná regido por regras de conduta similares àquelas aplicáveis a outros recursos de informática. O uso adequado deve ser legal, ético, refletir honestidade e demonstrar moderação no consumo dos recursos compartilhados. O uso inapropriado dos serviços de correio eletrônico, em alguns casos, pode causar interrupção das atividades da instituição.

As mensagens enviadas por meio do e-mail corporativo não são consideradas como informação particular. Assim sendo, a equipe de TI FUNEAS reserva para si o direito de monitorar e inspecionar o uso do e-mail disponibilizado, em conformidade com os termos da Lei.

Todas as mensagens ficam armazenadas em um servidor que possui recursos limitados.

Para que não ocorram problemas de indisponibilidade de caixas postais, o Colaborador deve periodicamente excluir as mensagens que não forem mais necessárias para liberar espaço na Caixa Postal e permitir que continue a receber mensagens.

A equipe de Tecnologia da Informação, não prestará suporte a outros e-mails com domínio (gmail, outlook, Hotmail entre outros), no entando a equipe prestará suporte para que o e-mail EXPRESSO @funeas.pr.gov.br, seja direcionado para outras caixas.

Não há qualquer procedimento específico (desativação, exclusão, etc.) para casos de ausência temporária (férias, licença-prêmio, licença sem vencimento, etc.).

Caixa postal para cargos em comissão e concursados FUNEAS terá a identificação no domínio FUNEAS com o seguinte exemplo:

nome.ultimo_nome@funeas.pr.gov.br

Caixa postal para terceiros terá a identificação no seguinte exemplo:

nome.ultimo_nome.ext@funeas.pr.gov.br

Caso exista o nome similar em outro órgão, será identificado pelo valor numérico iniciado por 1 e assim por diante, caso o login não permita a criação do email, conforme o exemplo:

nome.ultimo_nome1@funeas.pr.gov.br

nome.ultimo_nome2@funeas.pr.gov.br

É fundamental que o usuário que necessite acessar a internet nos computadores fornecido pelo FUNEAS, tenha o acesso à conta de e-mail para acesso ao proxy (páginas da internet)

Os colaboradores demitidos ou afastados terão a caixa postal bloqueada imediatamente e no período de até 6 (meses) meses a mesma será desativada ou excluída completamente para casos de desligamento, válido somente para o domínio @funeas.pr.gov.br.

Não obstante é expressamente proibido aos colaboradores:

- Transmitir material que seja considerado ofensivo, discriminatório, calunioso, fraudatório, danoso, ilegal ou que possa violar os padrões de ética e cortesia profissional;
- Transmitir ou abrir material que contenha pornografia e conteúdo de assédio moral;
- Transmitir piadas e conteúdo humorístico;
- Transmitir arquivos executáveis como anexo e extensões que possibilitem a propagação de vírus: (.bat, .chm, .cmd, .dll, .dot, .elm, .exe, .hta, .inf, .js, .jse, .lnk, .pif, .scr, .vbs, .vxd). Esta lista está sujeita a alterações sem aviso prévio;
- Retransmitir e-mails atachados com anexos não relacionados ao conteúdo

corporativo, os quais podem interromper ou prejudicar o funcionamento dos servidores/equipamentos de outra pessoa ou causar problemas de performance no sistema. Lembrando que não é possível o tráfego de e-mails com tamanho superior a 25MB;

- Abrir arquivos atachados de origem duvidosa;
- Colocar seus e-mails em chats e listas de discussão não relacionadas ao trabalho;
- Colocar as suas opiniões pessoais como sendo aquelas da FUNEAS;
- Divulgar informações consideradas confidenciais ou proprietárias da FUNEAS ou de suas unidades geridas, exceto quando aprovadas formalmente pela diretoria.
- Divulgar o endereço de e-mail de outros funcionários sem a anuência dos mesmos.

AFUNEAS se reserva o direito de preservar seus equipamentos e recursos computacionais através da recusa do recebimento de mensagens cujos conteúdos não expressam o interesse da FUNEAS, ou que possam colocar em risco o funcionamento dos sistemas.

As caixas postais do correio eletrônico, incluindo as informações contidas em seus arquivos, são propriedade da FUNEAS, reservando-se ao mesmo, portanto, o direito de monitorar e gravar toda a atividade quando considerar necessário. O uso da caixa postal de correio eletrônico e dos demais recursos de informática indica o consentimento do usuário a essa monitoração e, quando necessário, à divulgação da FUNEAS às autoridades competentes de quaisquer evidências que possam constituir crime, delito ou violação às atividades.

A FUNEAS poderá eventualmente realizar monitoração (auditoria) das caixas postais através da utilização de softwares específicos.

Todas as mensagens são passíveis de monitoração e gravação quanto aos endereços de destino e origem (IP de origem, E-mail do remetente, IP de destino, E-mail do destinatário) e poderão ser usados para estabelecer critérios de recusa. Eventuais ações de leitura de e-mail pela administração do sistema podem ocorrer perante autorização do responsável pela caixa postal ou do gestor. Para os casos de falha ou incompletude dos procedimentos previstos, bem como, no enfrentamento de situações inesperadas, a área de Tecnologia da Informação poderá, a seu critério, suspender a conta de correio ou todo o serviço comunicando o fato à Diretoria.

6.4 Acesso Físico e Lógico

Os colaboradores da FUNEAS devem ter acesso físico e lógico liberado somente aos locais e recursos necessários ao desempenho de suas atividades e de conformidade aos interesses da empresa.

A FUNEAS não possuo o seu Datacenter, o mesmo é alocado na CELEPAR e fornecido

como serviço pela Secretária de Saúde do Paraná.

O espaço da sala de tecnologia da informação é um ambiente isolado e deve ter acesso apenas pessoas autorizadas. Casos de manutenção e limpeza, um colaborador da Tecnologia da Informação deverá acompanhar.

O acesso à rede interna somente será realizado por meio das estações de trabalho, sendo que esses equipamentos serão controlados para eliminar possíveis riscos de vulnerabilidades, vírus e garantindo o cumprimento da política de utilização de softwares.

O procedimento formal de registro, mudança de colaborador de departamento/área e cancelamento de usuário para obtenção, alteração de privilégio e remoção de acesso a todos os sistemas de informação, a rede corporativa, bases de dados e a serviços necessários para o bom desempenho de sua atividade é realizado por meio de comunicado do setor de Recursos Humanos, conforme as informações descritas no e-mail encaminhado ao departamento de Tecnologia da Informação, assegurando a segregação de funções e a segurança da informação.

Para acesso aos equipamentos e sistemas aplicativos ligados à rede da FUNEAS, cada usuário deverá identificar-se por meio de senha. A senha é de uso pessoal e intransferível. Para que haja maior segurança nas estações de trabalho, o usuário deverá observar as seguintes determinações:

Toda vez que for se ausentar da sua mesa de trabalho, o usuário deverá, preferencialmente, bloquear sua estação da seguinte forma:

- Pressionar, ao mesmo tempo, as teclas “CRTL+ALT+DEL”;
- Clicar na opção “Bloquear computador” ou pressionar ao mesmo tempo a Tecla “WINDOWS + L”.

Todo equipamento que permanecer sem utilização por 20 (dez) minutos seguidos será automaticamente bloqueado e a proteção de tela ativada, salvo em estações de usuários com privilégios específicos.

A data e hora das estações de trabalho não poderão ser alteradas pelos usuários, sendo estas sincronizadas com os servidores automaticamente.

Qualquer componente de hardware do equipamento de cada usuário só poderá ser instalado, trocado ou removido pela área de Tecnologia da Informação. Os usuários somente poderão utilizar os softwares instalados pela área de Tecnologia da informação, não podendo instalar novos, alterar ou remover os existentes.

Os desktops deverão ser desligados pelos usuários após o seu expediente de trabalho, garantindo assim a conservação física e lógica, bem como a prevenção, no caso de ocorrência de algum problema elétrico ou na manutenção da rede.

A área de Tecnologia da Informação (administrador da rede LAN e/ou seus prepostos)

deverá efetuar o controle de acesso, de acordo com os privilégios definidos, por meio do Sistema de Administração da Rede, bem como a manutenção do cadastro dos colaboradores através da informação da área de Recursos Humanos sobre as movimentações (desligamento e transferências) de colaboradores.

Os registros de acesso somente poderão ser acessados pelo administrador da rede e/ou seus prepostos. A área de Tecnologia deverá instalar em todos os equipamentos, antes de sua utilização pelo usuário, softwares de detecção e proteção contra “vírus” (vacinas).

6.5 Senha de Acessos

Toda senha é de caráter pessoal, secreta e intransferível. Cada usuário é inteiramente responsável pela guarda e utilização de sua senha.

O compartilhamento de senhas será considerado como falta grave e passível de sanções disciplinares. Neste caso, a área de Tecnologia da Informação efetuará o bloqueio do acesso e comunicará a Diretoria.

As senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a rede ou a um sistema de informação ou serviço.

Para nenhuma finalidade é permitida a utilização de programas maliciosos para descobrir ou quebrar senhas de arquivos e programas.

A senha deverá ser alterada a cada 90 (noventa) dias corridos, sendo que a mesma não poderá ser repetida nas próximas 5 (cinco) alterações. Não obstante, o colaborador poderá alterar a sua senha, a qualquer momento, não sendo necessário aguardar os 60 (sessenta) dias entre as trocas.

A formação da senha deverá ser efetuada pelo próprio Colaborador, sendo composta por:

- No mínimo, 8 (oito) caracteres de comprimento;
- Bloqueio da Senha após 3 (três) tentativas. O desbloqueio será efetuado somente pela Tecnologia da Informação no ramal 2862.

Para a formação da senha, o usuário deverá tomar alguns cuidados para que não seja facilmente identificada por terceiros, como por exemplo, não utilizar:

- Nomes de cônjuges;
- Nomes de filhos;
- Data de nascimento;
- Anagramas (palavra ou frase formada pela transposição das letras de outra);
- Palavra ou frase, exemplo, Belisa (Isabel), Avalor (Álvaro), Arima (Maria);
- Números de documentos pessoais;
- Nunca usar uma senha igual ao nome do usuário.

Após a formação da senha, a mesma deverá ser memorizada pelo usuário. É expressamente proibida a impressão ou manutenção da senha anotada, assim como a

divulgação da mesma a terceiros.

A área de Tecnologia não pode solicitar e não necessita de sua senha para realizar qualquer atendimento. O equipamento deverá estar debloqueado com a senha do usuário e todo o tempo o usuário deverá acompanhar o atendimento.

6.6 Utilização de Software

A FUNEAS concede a seus colaboradores, juntamente com os servidores, desktops, notebooks e demais recursos disponíveis do seu patrimônio, a concessão de utilização de softwares, devidamente licenciados para o desempenho de suas atividades.

Todo software utilizado pelo FUNEAS tem seu direito de uso devidamente licenciado de terceiros.

Com relação ao uso em redes ou em máquinas multiusuários, os colaboradores da FUNEAS somente deverão usar o software de acordo com a licença acordada. O número de cópias simultaneamente em uso não poderá ultrapassar o contratado com o fornecedor.

A contratação de serviços correlatos à Tecnologia, sob qualquer pretexto, tem que ser previamente submetida à análise dos departamentos Jurídico e de Tecnologia da Informação. Somente é permitida a utilização de softwares homologados e licenciados através da área de Tecnologia da Informação.

Caso ocorra alguma necessidade de utilização de algum software que não esteja homologado, deverá ser solicitada a área de Tecnologia da Informação, na qual todos os procedimentos de homologação e legalização serão realizados.

Fontes, imagens gráficas, programas free como Adobe, Pkzip, Babylon, Imposto de Renda são considerados softwares, devem ser homologados e terem os direitos de uso autorizados pela área de Tecnologia Informação.

A área de Tecnologia da Informação é responsável por:

- Avaliar a necessidade de aquisição de softwares, bem como a sua compatibilidade;
- Proceder à instalação dos softwares adquiridos pela FUNEAS;
- Efetuar a transferência de software entre áreas ou entre computadores da mesma área;
- Acompanhar, juntamente com o usuário, o prestador de serviço, quando de atualizações de software/hardware, apresentações de novos aplicativos etc.

A FUNEAS reserva para si o direito de realizar inventários em seus ativos. Considerando que a Lei nº 9.609/98, disciplinou a proteção da propriedade intelectual sobre programas de computador, todos os deverão observar rigorosamente o disposto nesta lei, sob pena de incidirem nas sanções previstas na aludida norma federal.

Os colaboradores FUNEAS que identificarem alguma irregularidade no uso de software ou

na respectiva documentação deverão notificar a área de Tecnologia da Informação.

6.7 Utilização de Computadores e Notebooks

A FUNEAS e suas unidades geridas disponibiliza a cada colaborador um equipamento para uso individual. De acordo com as funções de cada área, este equipamento pode ser um desktop. Estes equipamentos fazem parte do patrimônio da FUNEAS e suas unidades geridas e é expressamente proibido retirá-lo das dependências da empresa, com exceção daqueles destinados a esta finalidade.

Os equipamentos compostos por uma estação de trabalho são:

1 – Gabinete (torre)

1 – Teclado

1 – Mouse

1 – Montior

- Todos os sistemas operacionais e sistemas necessários para execução de um bom trabalho.

Caso necessite de monitores secundários, a equipe de Tecnologia da Informação verificará a disponibilidade no seu estoque e ficará por competência da mesma disponibilizá-lo ou não para o usuário.

A mudança de localidade dos equipamentos, deve ser realizada pela equipe de Tecnologia da Informação do FUNEAS.

Caso ocorra o desligamento do colaborador, à área de Tecnologia da Informação fará a remoção do equipamento, para formatação e destinará para um novo usuário.

Qualquer notebook/desktop pessoal ou de visitantes da empresa não poderá adentrar a rede corporativa da FUNEAS. Toda mídia de origem externa como por exemplo pen drive, DVD, etc... deve ser submetida à área de Tecnologia da Informação antes de ser conectado nos equipamentos para que seja feito um Scan contra ameaças como vírus e etc.

6.8 Política de Gestão de Mudanças (GMUD)

O processo de Gestão de Mudanças definido conforme documento “Gerenciamento de Mudanças” baseado em ITIL.

Toda mudança e atualização de sistema deve ser planejada, aprovada pela área de negócios e pelo setor de Tecnologia da Informação FUNEAS, e executada na data e horário programado.