CARTILHA

TELETRABALHO COM SEGURANÇA

ASSESSORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (ATIC)

AFJP

O objetivo desta cartilha, elaborada pela Assessoria de Tecnologia de Informação e Comunicação (ATIC) da Fundação João Pinheiro (FJP), é orientar e facilitar os procedimentos do uso de ferramentas e tecnologias na rotina do teletrabalho, além de garantir um ambiente virtual seguro.

Todo o conteúdo é resultado de pesquisa interna entre os servidores da FJP sobre suas principais dificuldades no trabalho remoto.
Entre adaptações desta nova rotina, é fundamental que todos estejam alinhados com tais orientações.
Leia com a atenção e consulte esta cartilha sempre que for necessário.

No caso de dúvidas e sugestões, contato: atic@fjp.mg.gov.br

COMO GARANTIR A SEGURANÇA DA INFORMAÇÃO EM TELETRABALHO?

Processos seguros no acesso remoto

- Invista nas senhas e em criptografia (senhas apropriadas, que envolvem símbolos e a mistura de letras maiúsculas e minúsculas).
- Mantenha barreiras de proteção (antivírus/firewall).
- Atualize regularmente programas e softwares.

Cuidados com o notebook

- Transporte seguro: sempre na maleta/mochila.
- Na limpeza, menos é mais: utilize um tecido úmido sem produto químico.
- Mantenha o fio do carregador organizado.
- Comida e notebook não combinam. Se acidentalmente cair algo, limpe com um pincel e não deixe acumular. No caso de água, desligue, vire o equipamento de ponta-cabeça e espere escorrer totalmente.

Cuidados com o notebook

- Benjamim, a melhor companhia. Muitos carregadores de notebook possuem três pinos, o que dificulta sua adaptação numa tomada de dois. Nem pense em arrancar esse terceiro pino, pois ele não é inútil. Sem ele, você fica sem aterramento, que é o responsável por evitar que seu equipamento receba oscilações da corrente elétrica e inclusive você tome choque.

RISCOS AO COMPARTILHAR INTERNET

VELOCIDADE

Prejudica a velocidade contratada

SEGURANÇA

Problemas em relação à segurança de dados

JUSTIÇA

Problemas judiciais. Já imaginou se a pessoa com quem você compartilhou a sua senha cometer algum crime virtual, como a pedofilia?

Segurança com a rede wi-fi

- Defina uma senha.
- Altere o login e senha do roteador (a cada 3 meses).
- Ative o firewall do roteador.

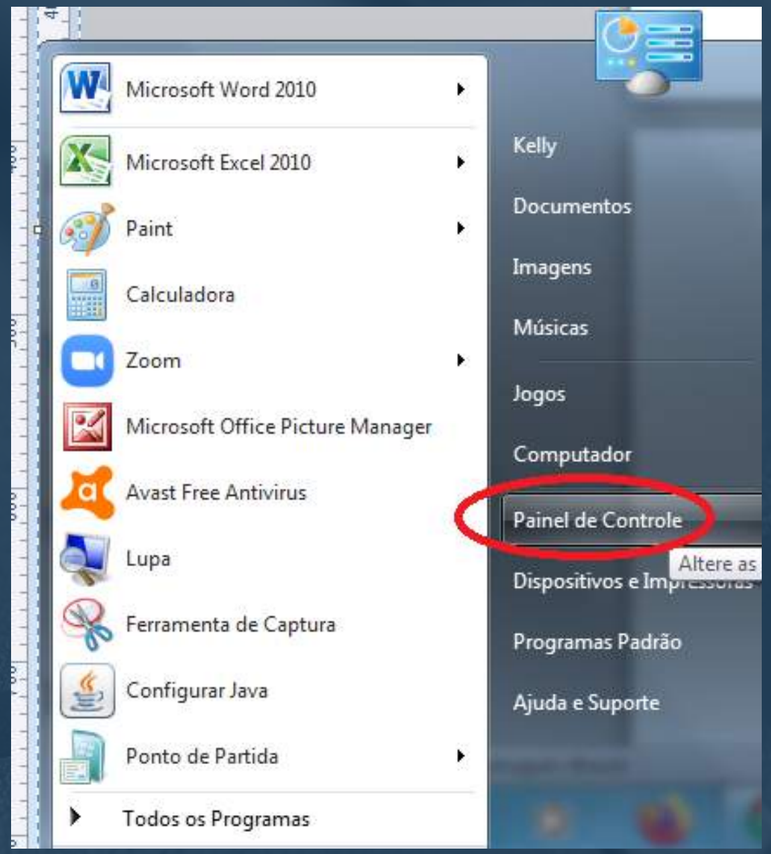
CONFIRA ATIVAÇÃO DO FIREWALL

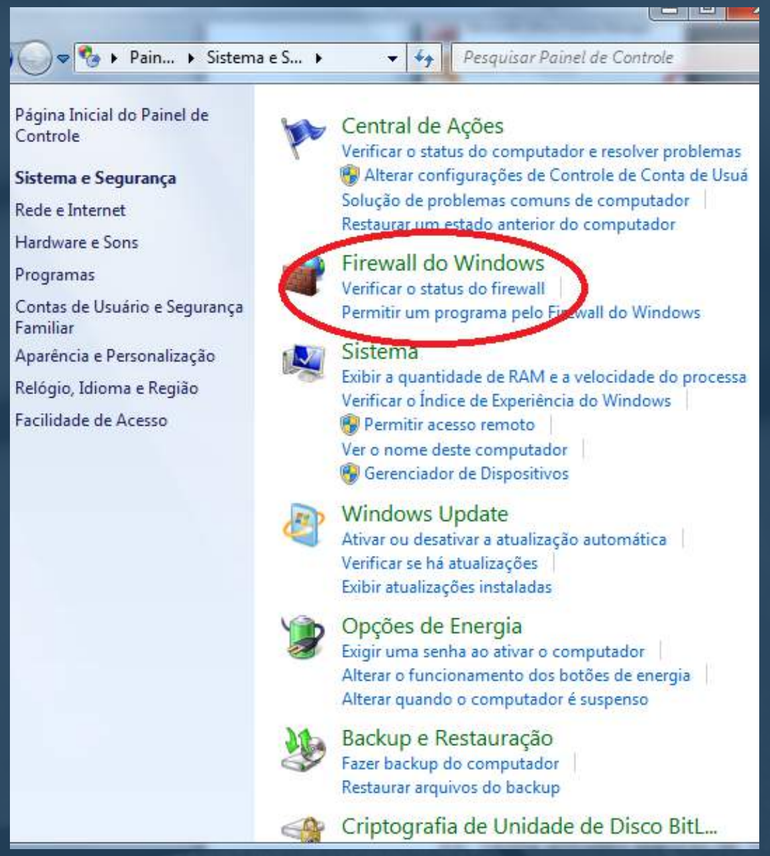
Certifique-se de que o seu firewall está ativado para manter seu computador em segurança.

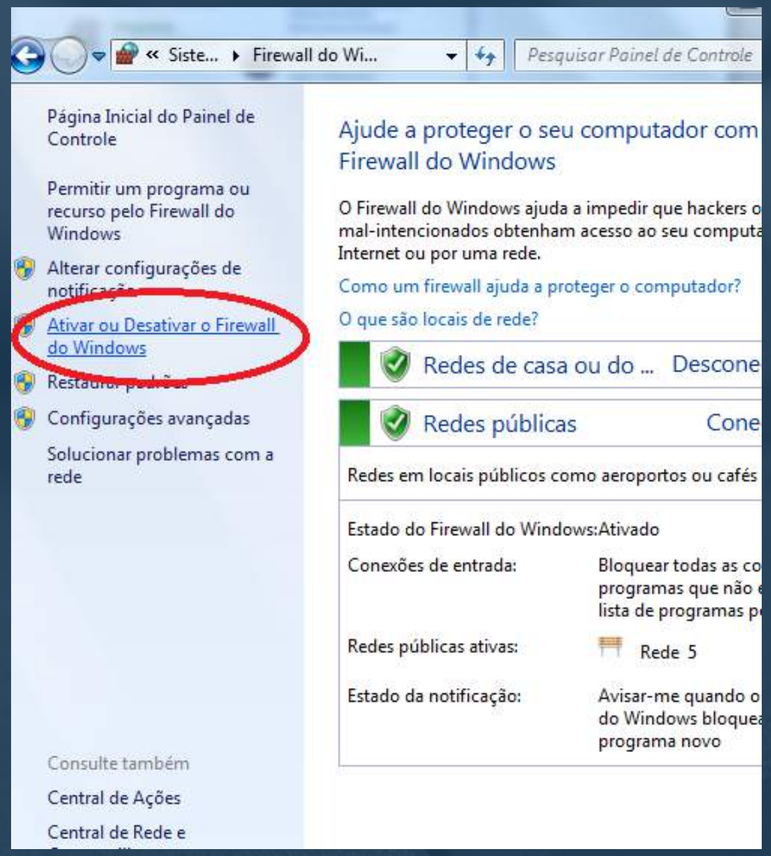
Em informática, um firewall (em português: parede de fogo) é um dispositivo de uma rede de computadores na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Para ver se o Firewall no Windows está rodando:

1. Clique no botão Iniciar do Windows e selecione Painel de Controle. A janela Painel de controle aparecerá.
2. Clique no link Central de Segurança. A Central de Segurança aparecerá.
3. **Se** no cabeçalho do **Firewall** diz **ATIVADO**, o **Firewall** no Windows **está** rodando.



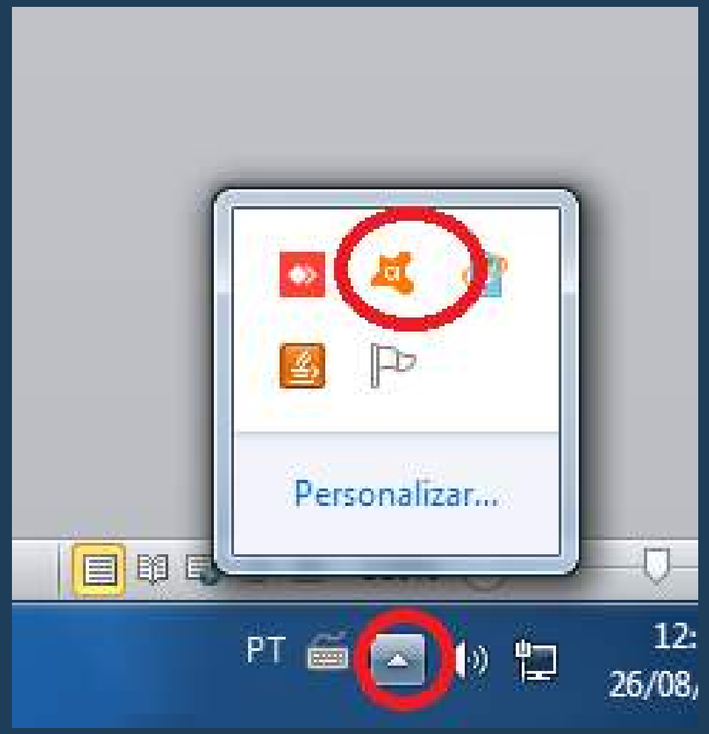

Pain... ▸ Sistema e S... ▸
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Sistema e Segurança
Rede e Internet
Hardware e Sons
Programas
Contas de Usuário e Segurança Familiar
Aparência e Personalização
Relógio, Idioma e Região
Facilidade de Acesso
Central de Ações
Verificar o status do computador e resolver problemas
Alterar configurações de Controle de Conta de Usuá
Solução de problemas comuns de computador
Restaurar um estado anterior do computador
Firewall do Windows
Verificar o status do firewall
Permitir um programa pelo Firewall do Windows
Sistema
Exibir a quantidade de RAM e a velocidade do processa
Verificar o Índice de Experiência do Windows
Permitir acesso remoto
Ver o nome deste computador
Gerenciador de Dispositivos
Windows Update
Ativar ou desativar a atualização automática
Verificar se há atualizações
Exibir atualizações instaladas
Opções de Energia
Exigir uma senha ao ativar o computador
Alterar o funcionamento dos botões de energia
Alterar quando o computador é suspenso
Backup e Restauração
Fazer backup do computador
Restaurar arquivos do backup
Criptografia de Unidade de Disco BitL...


« Siste... ▸ Firewall do Wi...
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Permitir um programa ou recurso pelo Firewall do Windows
Alterar configurações de notificação
Ativar ou Desativar o Firewall do Windows
Restaurar padrões
Configurações avançadas
Solucionar problemas com a rede
Ajude a proteger o seu computador com Firewall do Windows
O Firewall do Windows ajuda a impedir que hackers o
mal-intencionados obtenham acesso ao seu computa
Internet ou por uma rede.
Como um firewall ajuda a proteger o computador?
O que são locais de rede?
Redes de casa ou do ... Descone
Redes públicas Cone
Redes em locais públicos como aeroportos ou cafés
Estado do Firewall do Windows: Ativado
Conexões de entrada: Bloquear todas as co
programas que não
lista de programas p
Redes públicas ativas: Rede 5
Estado da notificação: Avisar-me quando o
do Windows bloquea
programa novo
Consulte também
Central de Ações
Central de Rede e

Altere a senha padrão do roteador

Acesse: Como mudar a senha do wi-fi pelo celular

Verifique se seu antivírus está operando



FERRAMENTAS DE SEGURANÇA

ANTIVIRUS/ANTISPYWARE/ANTISPAM

Software de segurança da informação

FIREWALL

Monitora e filtra os fluxos de tráfego em uma rede, identificando conexões inseguras ou possíveis ameaças à segurança do usuário

FERRAMENTAS PARA MANTER SOFTWARES DE TRABALHO ATUALIZADOS

IOBIT SOFTWARE UPDATER

Ferramenta gratuita que oferece uma forma simples de manter os programas instalados no computador atualizados.

KASPERSKY SOFTWARE UPDATER

É possível baixar a versão gratuita do programa e usá-lo para atualizar automaticamente os programas instalados no computador.

PATCH MY PC

Outro atualizador de programas gratuito para atualizar os programas no computador.

FERRAMENTAS PARA MANTER SOFTWARES DE TRABALHO ATUALIZADOS

SUMO (SOFTWARE UPDATE MONITOR)

Provavelmente um dos melhores programas gratuitos para verificar se existem atualizações para os programas no computador.

APPGET

Ferramenta gratuita para Windows que lhe permite instalar e atualizar os programas no computador por meio do Prompt de Comando

PROTEJA A WEBCAM

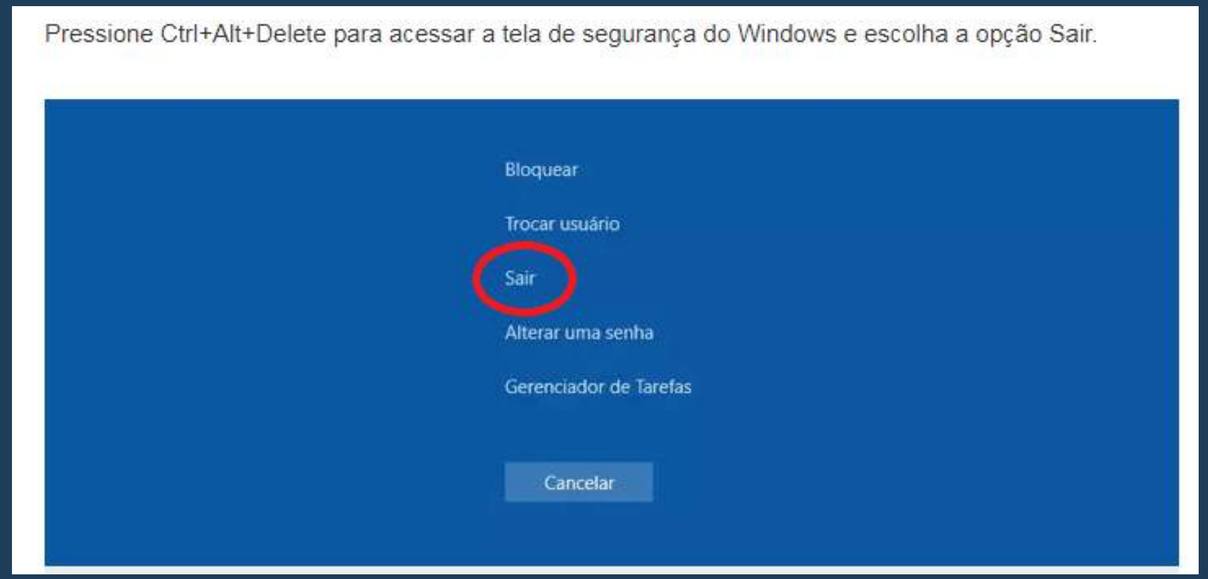
Se você utiliza um computador cuja câmara fica separada do monitor, remova o cabo que a conecta à máquina sempre que não estiver usando. Dessa maneira, o dispositivo fica seguro enquanto você não utiliza o equipamento.

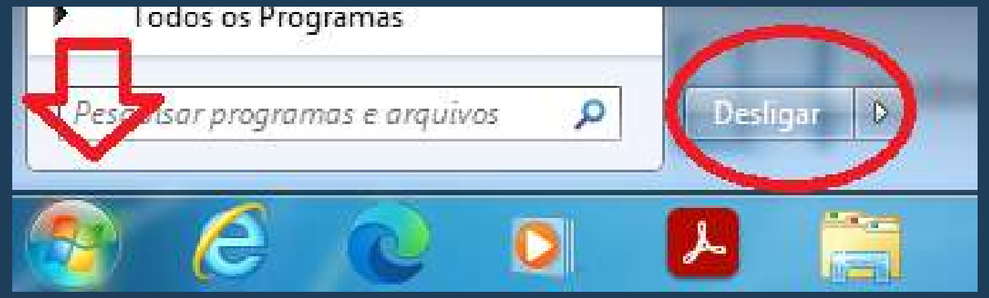
Cubra a webcam com uma fita isolante ou com um adesivo. Isso evita que ela seja acessada remotamente ou que suas informações vazem na internet.

Uma dica indispensável para quem procura manter a seu webcam segura é evitar o acesso a sites perigosos.

Outra medida para manter a segurança de seu webcam é desligar o dispositivo através do sistema operacional. Para fazer isso, basta desativar o seu suporte de driver.

DESLIGUE O COMPUTADOR APÓS O USO





AUMENTE, E ALTERE CONSTANTEMENTE, A SEGURANÇA DE SENHAS INSTITUCIONAIS

Uma senha é forte quando tem uma considerável extensão e possui símbolos, letras maiúsculas e minúsculas e inclusive números, ou seja, quando está fora da lista de piores senhas habituais como '123456' ou 'password'.

Nunca forneça senhas e duvide de pedidos incomuns de pessoas conhecidas.

MANTENHA DUPLA VERIFICAÇÃO (AUTENTICAÇÃO)

A verificação dupla – também chamada de autenticação de dois fatores – é uma forma de proteger a sua conta em serviços online caso a sua senha tenha sido roubada.

Para ativar a autenticação em dois fatores é necessário entrar nas configurações da sua conta. Ou seja, no site ou aplicativo é preciso verificar no local ou aba “segurança” se existe esta função. Caso a mesma esteja disponível, basta seguir as orientações para configurar.

DISPOSITIVOS E PÁGINAS

Somente utilize dispositivos de armazenamento externo (pen drive, HD externo) após passar o antivírus.

Somente acesse dispositivos autorizados (páginas seguras): use sempre conexões seguras, como "HTTPS" para acesso a sites web e remoto.

BACKUP

Faça backup dos seus dados e ative backup automático em repositório de arquivos em nuvem.

Fazer o backup dos seus dados protege sua informação no caso de uma pane no computador ou falha elétrica. Também ajuda se você cair na armadilha de um ransomware, que criptografa os seus dados confidenciais.

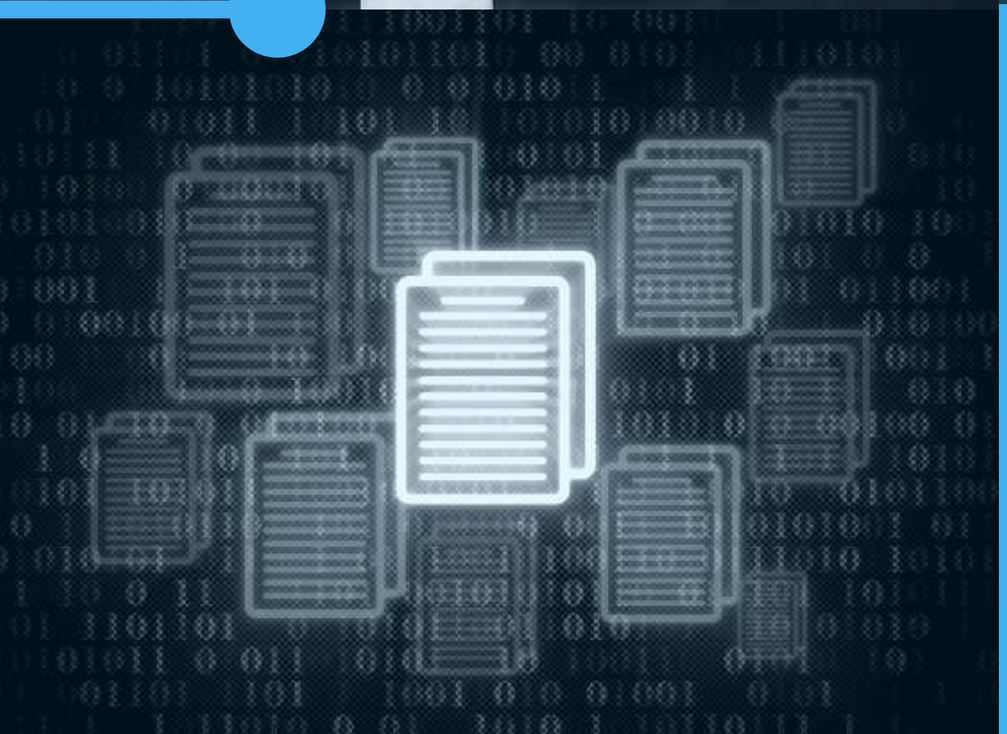
Na FJP, deve-se ter um sistema de backup atualizado e fortemente robusto para ter a capacidade de armazenar e recuperar todo o acervo de informações da instituição.

BACKUP

1. **Backup** no computador. Uma das formas mais simples e rápidas de **fazer** um **backup** é com mídia física, gravando os **dados** em CD, DVD e Blu-ray. ...
2. Através do pendrive. ...
3. HD externo pode ser uma boa opção. ...
4. Arquivos na nuvem. ...
5. **Backup** em dispositivos móveis. ...
6. Verifique **seus** arquivos após **fazer** o **backup**.

POLÍTICA DE COMPARTILHAMENTO DE ARQUIVOS

Combine com a sua chefia o que pode ser compartilhado com outros setores.



ALERTA

Investigue indícios de comprometimento do dispositivo (computador e internet lenta etc.)

Mantenha atualizados os contatos de servidores que atuam na ATIC.

E-MAILS

Não abra e-mails, anexos ou hiperlinks duvidosos.

Não abra e-mails de desconhecidos.

As mensagens sempre deverão incluir assinatura padrão:

- Nome do colaborador
- Gerência ou departamento
- Nome da instituição
- Telefone(s)

E-MAILS

Não responda a e-mails que solicitam recadastramento de senhas, dados de conta bancária e de cartão de crédito, prêmios, promoções, sorteios, brindes, informações pessoais, informações confidenciais, documentos de identidade, CPF e outros que pareçam suspeitos.

USO DA INTERNET

- Assegure-se de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.
- Tome cuidado com sites de estações de rádio, TV, jogos e filmes, mesmo por meio de dispositivos USB; de conteúdo pornográfico ou correlato; que defendam atividades ilegais; que menosprezem, depreciem ou incitem o preconceito a determinadas classes; que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da FJP; que promovam discussão pública sobre os negócios da FJP, a menos que autorizado pela diretoria; que possibilitem a distribuição de informações de nível confidencial; que permitam a transferência (downloads) de arquivos e/ou programas.

TENHA ATITUDES SEGURAS DE TI

E qualquer situação adversa, acione a ATIC.
e-mail: atic@fjp.mg.gov.br

FJP
FUNDAÇÃO JOÃO PINHEIRO

Redação: KELLY REGINA MARTINS MILHORATO (ATIC)
Revisão e aprovação: THIAGO SANTOS DE MIRANDA NUNES (ATIC)
Revisão e diagramação - TIAGO ALVES DA SILVA (ACS); DÉBORA DRUMOND (ACS)
Apoio: RENATA GRACIELA MOREIRA CARDOSO (ATIC); DENILSON RODRIGUES MARTINS (ATIC)

FJP
FUNDAÇÃO JOÃO PINHEIRO