Coordenadoria de Tecnologia da Informação e Comunicações - CTIC

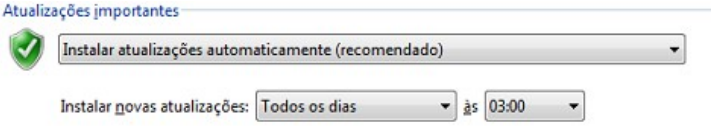
Governança de TIC
CGOV

Segurança da Informação
SSI

Proteja-se!

Edição extraordinária para o servidor em regime de teletrabalho

Sempre instale as últimas atualizações e correções de segurança disponíveis



Softwares mal-intencionados são lançados a todo o momento, podendo utilizar as vulnerabilidades de um sistema operacional não atualizado, danificando e obtendo acesso não autorizado aos dados no computador.

As atualizações, em especial as do Windows, corrigem a maior parte das vulnerabilidades.

Utilize somente sistema operacional e programas licenciados

Um programa/sistema operacional não licenciado pode expor seu computador a uma série de problemas de segurança, afetando o desempenho e comprometendo sua privacidade.
Para burlar os processos de licenciamento, usuários fazem uso de programas chamados de *crack*.

No entanto, não há garantia de que elas não tenham sido desenvolvidas para aproveitar o acesso a recursos administrativos do computador, para instalar algum tipo de *malware* durante a execução, e isso é o que normalmente ocorre.

O licenciamento do sistema operacional e demais programas instalados na estação de trabalho doméstica do usuário é de **sua inteira responsabilidade**.

Mantenha o antivírus atualizado

Manter o antivírus atualizado é importante para trazer defesas às novas ameaças que vão surgindo diariamente na internet.

As ameaças descobertas são analisadas minuciosamente e enviados aos fabricantes de soluções de segurança, para que possam disponibilizar novas proteções aos seus usuários.

Clique AQUI para acessar as informações sobre a Segurança da Informação

Caso tenha alguma dúvida, sugestão ou crítica envie para cati@trt16.jus.br

Coordenadoria de Tecnologia da Informação e Comunicações - CTIC

Governança de TIC
CGOV

Segurança da Informação
SSI

Proteja-se!

Edição extraordinária para o servidor em regime de teletrabalho

Habilite o *Firewall* do Windows

O *Firewall* tem a capacidade de permitir ou não o tráfego de determinadas conexões entre o seu computador e a internet.

Ele atua impedindo que pessoas ou aplicações não autorizadas adentrem, visualizem, roubem ou danifiquem os dados.

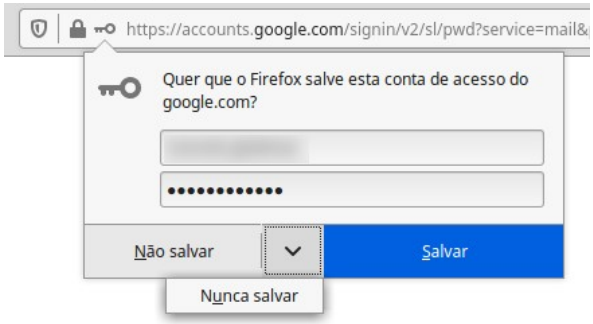
Não exponha dados e informações sensíveis do TRT16 a terceiros

As informações confidenciais do TRT16, se vazadas, podem comprometer seriamente o órgão, por exemplo, causando danos à reputação e imagem do Tribunal, prejuízos financeiros, e ainda, comprometimentos legais.

Não mostre documentos a familiares, prestadores de serviço, entre outros.

Não deixe documentos impressos no local de trabalho.

Não anote ou salve as senhas de acesso ao ambiente de teletrabalho nos navegadores ou outros programas



Um dos problemas em permitir que um navegador salve suas senhas é a utilização do mesmo computador por outra pessoa, que poderá acessar os sistemas e informações sem autorização.

Existem os riscos de **vazamento de informações**, **roubo de dados**, **sequestro de dados**, **inclusão**, **alteração** ou **exclusão de dados**, **invasão de sistemas**, entre outros.

Os níveis dos riscos aumentam no caso de perda ou roubo do equipamento utilizado em regime de teletrabalho.

Nesse sentido, é preciso ter muito cuidado e atenção para evitar o salvamento de senhas em navegadores, pois além dos riscos supracitados, alguns vírus e *softwares* maliciosos – *malwares* podem ter a capacidade de roubar estas informações de modo transparente para o usuário.

É sempre bom lembrar que no caso de descarte de dispositivos de armazenamento (HDs, *pendrives*, cartões de memória, etc) e de equipamentos (computadores *desktop*, *notebooks*, *tablets*, *smartphones*, etc), é importante apagar as informações gravadas.

Por fim, não deixe senhas anotadas em papéis no ambiente de teletrabalho.

Clique AQUI para acessar as informações sobre a Segurança da Informação

Caso tenha alguma dúvida, sugestão ou crítica envie para cati@trt16.jus.br

Coordenadoria de Tecnologia da Informação e Comunicações - CTIC

Governança de TIC
CGOV

Segurança da Informação
SSI

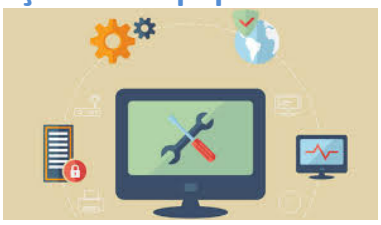
Proteja-se!

Edição extraordinária para o servidor em regime de teletrabalho

Cuidados com equipamento utilizado em teletrabalho

No caso de manutenção, descarte, perda ou roubo de equipamentos, é importante que as senhas de rede e de sistemas utilizados para teletrabalho sejam **alteradas imediatamente**.

Manutenção nos equipamentos



Caso seja necessária manutenção por terceiros em seu equipamento – computador, *tablet*, *smartphone* e outros –, recomenda-se:

- sempre que possível, realizar cópia dos arquivos do TRT16;

- após a cópia, excluir os arquivos para evitar a possibilidade de vazamento de informações;

- quando o equipamento retornar da manutenção, realizar a alteração das senhas.

Descarte de equipamentos

Ao descartar um equipamento, deve ser realizada prévia exclusão de todos os arquivos do TRT16. Recomenda-se ainda a remoção de todos os arquivos pessoais.

Perda de equipamentos

Em caso de perda de equipamento, se o dispositivo possibilitar um meio de rastreamento remoto, recomenda-se monitorar sua localização para recuperá-lo.

Em caso extremo, pelo rastreamento remoto, recomenda-se a exclusão dos arquivos para evitar vazamento ou acesso não autorizado.

Roubo de equipamentos

Em caso de roubo, são recomendadas as seguintes ações:

- registrar boletim de ocorrência junto à autoridade policial;

- caso exista meio de rastreamento do equipamento, monitorar sua localização e repassar as informações à autoridade policial.

Importante!

Tanto nas situações de **perda** ou de **roubo**, se não houver sucesso na recuperação do equipamento, recomenda-se, quando possível, bloqueá-lo.

Clique AQUI para acessar as informações sobre a Segurança da Informação

Caso tenha alguma dúvida, sugestão ou crítica envie para cati@trt16.jus.br

Coordenadoria de Tecnologia da Informação e Comunicações - CTIC

Governança de TIC
CGOV

Segurança da Informação
SSI

Proteja-se!

Edição extraordinária para o servidor em regime de teletrabalho

Segurança da rede doméstica

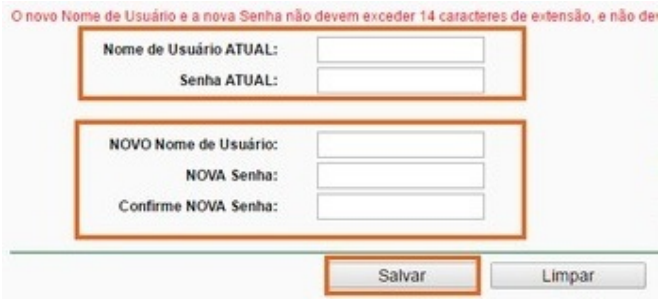
WPA2

A rede sem fio do TRT16 busca, na medida do possível, contar com as configurações mais seguras para os usuários.

Para ter um nível de proteção similar em sua casa, configure sua rede sem fio doméstica no modo mais seguro. O protocolo de segurança WPA2 é o mais indicado.

Para habilitar o modo WPA2, acesse as configurações de seu roteador.

Senha do equipamento de rede sem fio



A alteração da senha padrão do roteador sem fio representa a mais importante medida de segurança a ser implementada em uma rede doméstica.

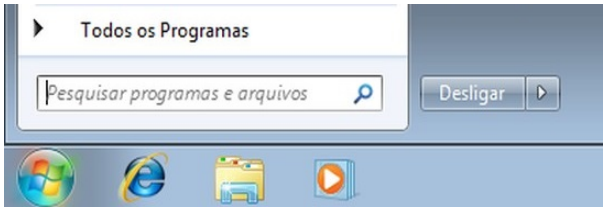
Senhas predefinidas são de conhecimento comum. Sem a alteração das senhas definidas pelo fabricante, o **risco de sofrer ataques torna-se demasiadamente alto**, comprometendo a **própria rede**, os **dispositivos conectados**, os **arquivos armazenados** e **trafegados**, os **dados pessoais**, as **credenciais de acessos a sistemas**, os **dados bancários**, os **dados e informações do TRT16** entre outros.

Para alterar a senha padrão do equipamento, acesse as configurações. Caso necessário, consulte o manual do dispositivo.

Bloqueio e desligamento do computador

Bloqueie o computador sempre que precisar deixar o escritório de casa, mesmo em ausências curtas.

No Windows, pressione as teclas **Windows + L** para bloquear o computador.



Desligue o computador sempre que encerrar as atividades de teletrabalho.

As duas práticas evitam que pessoas não autorizadas tenham acesso às informações do TRT16.

Clique AQUI para acessar as informações sobre a Segurança da Informação

Caso tenha alguma dúvida, sugestão ou crítica envie para cati@trt16.jus.br

Coordenadoria de Tecnologia da Informação e Comunicações - CTIC

Governança de TIC
CGOV

Segurança da Informação
SSI

Proteja-se!

Edição extraordinária para o servidor em regime de teletrabalho

Mais informações importantes!

Armazenamento de documentos corporativos

O armazenamento de documentos corporativos deverá ser feito exclusivamente nos locais adequados providos no ambiente de teletrabalho.

Essa medida visa garantir aos documentos utilizados em teletrabalho o mesmo nível de proteção dos documentos utilizados no TRT16.

Política de Segurança da Informação

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO
SECRETARIA DO TRIBUNAL PLENO

Protocolo nº 159-2016

RESOLUÇÃO Nº 202, DE 23 DE SETEMBRO DE 2016

A RESOLUÇÃO N° 202, DE 23 DE SETEMBRO DE 2019, que estabelece as diretrizes de segurança da informação e comunicação no âmbito do Tribunal que deve ser adotado por todos os usuários do TRT16. Clique AQUI para acessá-la.

Monitoramento e auditoria

O acesso realizado pelo ambiente de teletrabalho será monitorado e registrado pela CTIC, podendo a qualquer momento ser efetuada auditoria.

Clique AQUI para acessar as informações sobre a Segurança da Informação

Caso tenha alguma dúvida, sugestão ou crítica envie para cati@trt16.jus.br