BOAS PRÁTICAS EM TECNOLOGIA DA INFORMAÇÃO

TECNOLOGIA DA INFORMAÇÃO PRIMA EMPREENDIMENTOS INOVADORES

2022/2023

Rua Waldemar Falcão Nº 819 Ed. Prima Horto Florestal Salvador- Bahia – CEP 40.295-010
http://www.primainova.com.br

Sumário

GUIA BOAS PRÁTICAS EM TECNOLOGIA DA INFORMAÇÃO

POLÍTICAS DE USO DOS COMPUTADORES

1. Para que serve uma política de uso? Para estabelecer padrões e procedimentos que busquem a segurança, estabilidade e disponibilidade dos serviços computacionais.

2. Quais recursos computacionais devem seguir a política de uso? Quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital inseridos no ambiente computacional da Prima Empreendimentos Inovadores SA, incluindo notebooks, tablets, smartfone, pen drives, HD externos, impressoras, além das estações de trabalho.

3. O que posso instalar no computador? O setor de Tecnologia da Prima Empreendimentos distribui os computadores (estações de trabalho) instalados com sistemas e programas licenciados de acordo com o padrão adotado a partir do orçamento de 2022. Então, por razões de padronização e segurança, o usuário não pode instalar aplicativos e programas sem intervenção do setor de Tecnologia. Em caso de necessidade específica de algum programa ou sistema, deve-se entrar em contato com a Divisão de Tecnologia da Prima Empreendimentos para averiguar o possível licenciamento ou instalação caso seja software livre.

4. Que tipo de sítios posso acessar? Por motivos de segurança e disponibilidade do link de dados, o acesso aos sites está sendo filtrado para inibir acessos a conteúdos indevidos ou inadequados ao ambiente de trabalho. Em caso de necessidade de acesso a um sítio que esteja bloqueado, consulte a Divisão de Tecnologia sobre a possibilidade de liberação.

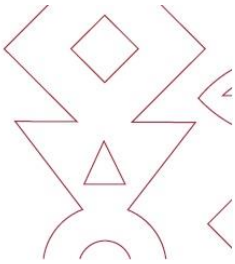
CUIDADOS PARA UTILIZAÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA DENTRO E FORA DO AMBIENTE CORPORATIVO

1. Não ligar o computador, impressora, fax, escâner, bebedouro, etc, na mesma tomada, seja usando extensões, no breaks, estabilizadores ou adaptadores elétricos. Caso isso ocorra será gerada uma sobrecarga elétrica podendo queimar um ou mais equipamentos e ocasionar princípio de incêndio;
2. Quando se perceber alterações na rede elétrica, deve-se salvar os documentos e por medida de segurança desligar os equipamentos por um período, até que a rede elétrica volte ao normal. As principais características de alterações na rede elétrica são: lâmpadas piscando ou com luminosidade fraca, constantes bips de no breaks ou estabilizador, várias interrupções no fornecimento de energia por um curto período de tempo;
3. Quando não for mais utilizar os equipamentos desligar normalmente e após isso retirar o plugue da tomada;
4. Ao ligar uma impressora aguarda o tempo necessário para o que o sistema de impressão seja carregado, o tempo médio é de 3 minutos, só após esse tempo se deve mandar os documentos para impressão;
5. O abastecimento da impressora com excesso de papel, pode causar o problema na tração dos roletes uma vez que podem se puxados mais de uma folha ao mesmo tempo, este mesmo problema pode ocorrer em caso de folhas úmidas, sempre que for abastecer com folhas verifique se as mesmas estão soltas;
6. Quando a impressora estiver por muito tempo sem uso, antes da impressão solte as folhas com a mão deixando-as separadas;
7. Quando ocorrer de uma folha ficar presa dentro da impressora, primeiro cancele o processo de impressão e desligue-a da rede elétrica antes de tentar remover a folha. Caso a remoção esteja exigindo muita força solicite a presença do técnico, remover uma folha pode causar desalinhamento em peças internas;
8. Não retirar e colocar de maneira brusca o tôner/cartucho da impressora, pode haver derramamento do pó/tinta de impressão ocasionando acúmulo de sujeira dentro do equipamento;

9. Toda impressora possui um tempo de espera para que o documento seja totalmente carregado em sua memória, somente após esse procedimento é que será impresso. Então o usuário deve enviar o arquivo para impressão e aguarda ele ser impresso, não adianta mandar duas ou três vezes o mesmo documento que ele não será impresso mais rápido, e sim consumir mais papel e tôner da impressora, caso o tempo de espera ultrapasse 2 minutos ai sim poderá ser considerado um problema e deve-se verificar: papel na impressora, tôner e papel preso, caso nenhum desses seja o problema procurar o setor de tecnologia para averiguação;
10. Não deixar os cabos que conectam a impressora, escâner ou o computador muito esticados ou mal encaixados;
11. Deixe o computador limpo, livre de poeira e umidade;
12. Em casos de relâmpagos, desligue o equipamento da tomada;
13. Evite fazer refeições na frente do computador;
14. Não conecte ou desconecte nenhum cabo com o computador ligado, exceto os cabos de rede e USB;
15. Não bata, empurre ou mude de lugar o computador com ele ligado, isso pode prejudicar o hardware do computador;
16. Não ligue e desligue o computador diversas vezes consecutivas, você pode danificar algum componente;

COMO UTILIZAR DE FORMA SEGURA O SISTEMA OPERACIONAL E APLICATIVOS

1. Quando utilizar um pendrive, câmeras digitais, celulares ou outros dispositivos conectados ao computador, a primeira coisa a fazer é uma varredura com o antivírus para eliminar programas maliciosos. Uma simples abertura do dispositivo sem os cuidados necessários é suficiente para infectar o computador com programas maliciosos, corromper arquivos e pastas do sistema deixando o computador inutilizável até os devidos reparos;



2. Não deixar que usuários não autorizados ou que não sejam do setor administrativo do campus utilizem os computadores e impressoras, pois se eles não possuírem conhecimentos para prevenir contaminação por vírus de computador ou manuseio de impressoras, poderão danificar os equipamentos ou o sistema operacional e acessar sites de conteúdo nocivos ao computador como: jogos, pornografia, software piratas, download de filmes e músicas. Prejudicando a utilização da rede de computadores para tarefas administrativas;
3. Sempre fazer o backup de seus arquivos de trabalho pelo ao menos uma vez por semana;
4. Nunca desligar o computador diretamente na tomada elétrica ou no botão de desligar, sempre utilizar o método tradicional do sistema operacional;
5. Não Clique em Links desconhecidos que você recebe pelo WhatsApp/E-mail etc;
6. Em suas senhas combine letras, números e caracteres especiais;
7. Nunca forneça suas senhas a ninguém;
8. Não clique em link recebido através de redes sociais, pois estes podem apontar para malwares e sites de phishing. Principalmente se este link vier de alguém desconhecido;
9. Nunca utilize senhas baseadas em informações pessoais;
10. Jamais clique em programas recebidos por e-mail cuja origem você desconhece;
11. Verifique com antivírus atualizado os arquivos recebidos por e-mail antes de executá-los;
12. A menos que você solicite, bancos nunca entram em contato com clientes através de e-mail, muito menos operadoras de cartões de crédito;
13. Desconfie de todas as mensagens recebidas por e-mail cujo conteúdo solicite informações ou atualizações de dados pessoais;
14. Não clique em URL de bancos recebidas por e-mail. Elas normalmente direcionam usuários para sites fraudulentos;
15. Acostume-se a sempre digitar manualmente no seu navegador o endereço (URL) do seu banco;

16. Em acessos a páginas da Internet que peçam login e senha. sempre verifique a presença do cadeado fechado no canto inferior direito do seu navegador.

SERVIÇOS DISPONIVEIS AOS USUÁRIOS

Como acessar o servidor de arquivos?

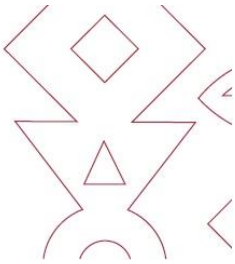
- Todo setor tem um espaço no servidor de armazenamento de dados para guardar arquivos. Durante o processo de autenticação da rede, o sistema mapeia automaticamente uma letra associada ao espaço correspondente ao seu setor. Esse espaço é exclusivo para alocar arquivos que fazem parte do trabalho. Não se deve armazenar, nesse local, arquivos de cunho particular ou arquivos do tipo, imagem, vídeos ou áudio. Necessidades específicas de armazenamento devem ser solicitadas junto ao setor de tecnologia, que será analisada a possibilidade de atendimento.

- A política de backup do servidor de arquivos é feita diariamente, portanto se o arquivo excluído foi criado no mesmo dia, é necessário uma ação de recuperação até as 22 horas do dia corrente, caso ultrapasse o tempo o arquivo poderá ser perdido completamente.

Como solicitar um equipamento?

- Para solicitar equipamentos de informática, o responsável pela setor deve encaminhar e-mail com o pedido para o setor de tecnologia.
- A solicitação deve ser detalhada para que o setor de tecnologia avalie a melhor configuração a ser utilizada.
- O atendimento do pedido também depende da disponibilidade e da adequação à política de tecnologia da informação da Prima Empreendimentos.

Como solicitar um suporte técnico?



- Atualmente está sendo desenvolvido um sistema para abertura de chamados de TI onde será realizado as aberturas e atendimentos somente através desse sistema.
- Atualmente as solicitações são feitas por telefone ou se dirigindo até o analista de TI, quando o sistema estiver homologado e em uso, as solicitações serão feitas unicamente e exclusivamente pela ferramenta, solicitações feitas fora do sistema dependerá da disponibilidade técnica dos servidores de TI;
- (Com o sistema em USO) Toda a troca de informações sobre o suporte técnico será feita através do sistema, via inserção de comentários;
- (Com o sistema em USO) Será de responsabilidade do usuário acompanhar o andamento de sua solicitação e fornecer informações quando solicitado;

SEGURANÇA DA INFORMAÇÃO

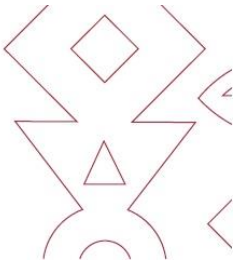
O que pode ocorrer com um computador vulnerável?

Entre outras coisas, pode ocorrer:

- Roubo de informação;
- Perda de dados;
- Redução de desempenho;
- Uso do computador para atacar servidores e outros computadores. Por isso, os cuidados com a segurança são importantes.

As Senhas são utilizadas para:

- Acesso a rede;
- Acesso à internet; •
- Acesso ao ERP `
- Impressão
- Além dessas, podem ser necessárias outras para acessar aplicativos específicos.



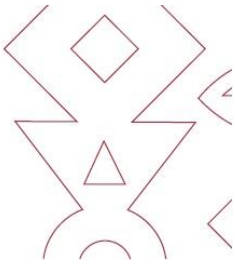
Como alterar minha senha? Para alterar suas senhas, veja os passos descritos a seguir para cada tipo de acesso:

- Acesso a rede e a internet 1. Pressione a combinação de teclas ctrl+alt+del; 2. Clique em “Alterar uma senha”; 3. Forneça a senha atual, nova senha e confirme a nova senha.
- Por razões de segurança, quando o sistema de monitoramento detecta algum tipo de atividade suspeita com o perfil de usuário, automaticamente o perfil é bloqueado. Neste caso, você deve Abrir um chamado (Quando o sistema estiver disponível) para o setor de Tecnologia e solicitar a liberação. Importante: somente o próprio usuário pode solicitar a liberação do acesso ou uma nova senha.
- Jamais compartilhe senhas com outras pessoas. Lembre-se que, a princípio, você é o responsável por tudo que ocorre com o uso de sua senha. • Se você não consegue memorizar suas senhas e precisa anotar em algum lugar, dificulte o acesso das pessoas aos seus lembretes. Não deixe suas senhas anotadas em locais visíveis, de fácil acesso, expostas em cadernos, pastas ou marcadores em sua mesa de trabalho.
- A senha existe para evitar acessos não autorizados por outras pessoas a ambientes e sistemas que exigem segurança e controle, por isso, bloqueie sempre o seu computador em suas ausências, evitando o acesso indevido a informações sob sua responsabilidade. No Windows, utilize o conjunto de teclas <Ctrl> +<Alt>+<Del> ou <Windows> + <L> para bloquear rapidamente o computador.
- Utilize senhas também em celulares e notebooks, protegendo suas informações em caso de extravio, furto ou roubo do equipamento.
- Sempre que possível diversifique as senhas que possui, evitando que a descoberta de uma delas dê acesso a outras informações protegidas.

PERGUNTAS

Quais os riscos ao navegar na internet?

Alguns sítios exploram vulnerabilidades dos navegadores e acabam instalando programas maliciosos no computador do usuário. Por isso, é importante manter os aplicativos atualizados e não fazer download de arquivos em sítios desconhecidos.



Programas Maliciosos São programas criados para executar ações maliciosas no computador, como captura de senhas e danificação de arquivos e programas. Os mais comuns são: Vírus – programa que infecta o computador utilizando-se de diversos meios. É replicado pela ação do computador infectado. Cavalo de troia – programa invasor que pode ler, copiar, apagar e alterar dados do sistema sem o conhecimento do usuário. Backdoors – programa que tenta obter controle de uma máquina aproveitando-se uma falha de segurança em um programa de computador ou sistema operacional, abrindo uma porta para seu invasor controlar o computador remotamente. Keylogger – programa capaz de capturar e armazenar as teclas digitadas pelo usuário.

O antivírus protege contra programas maliciosos?

Em geral, o antivírus detecta programas maliciosos oriundos de e-mails, CDs, cartões de memória, pen drives etc. Contudo, é sempre bom tomar cuidado com todas as mídias que recebe. Verifique sempre se o antivírus está funcionando e atualizado. Evite também executar programas ou abrir arquivos de origem duvidosa. Lembre-se que, por exemplo, joguinhos de computador aparentemente inofensivos, ao serem executados, poderão conter e instalar programas maliciosos, que poderão ocasionar danos irreversíveis aos seus arquivos, mau funcionamento do seu equipamento ou até mesmo furtar suas senhas. Muitas vezes, esses arquivos podem vir de amigos ou colegas de trabalho que desconhecem que seus arquivos possuem essa ameaça.

Recebi um e-mail solicitando minha senha, devo responder?

Não! Nunca se deve informar senhas e dados pessoais por e-mail. Há uma prática maliciosa conhecida como “phishing”, que consiste em solicitar informações ou ações do usuário. Cuidado, como essas mensagens se assemelham a e-mails verdadeiros, é possível o recebimento de algum e, por isso, deve-se estar sempre atento.

Recebi um e-mail solicitando divulgação de um fato, o que faço?

É comum algumas mensagens do tipo “Ajude essa criança com câncer” ou “Previna-se do novo vírus” solicitando divulgação (“envie para todos da sua lista”). A maioria dessas mensagens é boato e não deve ser passada adiante. Vários vírus são disseminados por meio de links em textos ou em fotos. Não se deve, portanto, abrir anexos ou links recebidos de remetentes desconhecidos.

Preciso fazer backup dos meus dados?

Sim. O Setor de Tecnologia é responsável pelo salvamento dos dados armazenados nos servidores. Quanto aos dados armazenados nas estações de trabalho, o próprio usuário é responsável pelo seu salvamento.

REDE SEM FIO

É uma rede que pode ser acessada sem a necessidade de conexões por fios metálicos. A mais comum utiliza radiofrequência na comunicação entre os computadores. Essa tecnologia é indicada quando se necessita de mobilidade, como no uso de notebooks. Embora a rede sem fio permita mobilidade, a rede com cabo é mais estável e mais rápida.

OS 10 MANDAMENDOS DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

1. Utilize senhas difíceis de serem descobertas;
2. Altere sua senha periodicamente;
3. Tome cuidado com downloads;
4. Tome cuidado com e-mails de remetentes desconhecidos;
5. Evite sítios com conteúdo duvidosos;
6. Não abra anexos de e-mails desconhecidos;
7. Tome cuidado com compras na internet;
8. Tome cuidado ao acessar sítios de bancos;
9. Não revele informações sobre você na internet;
10. Ao informar dados em sítios, verifique se a página é segura (com prefixo “https”).