MANUAL DE BOAS PRÁTICAS – ANTIVÍRUS ESET

Esse manual tem como objetivo auxiliar o usuário a obter o melhor do produto ESET e a melhor segurança para a (s) sua (s) máquina (s). Esse documento consiste em diversas técnicas que aprimoram a sua proteção durante a sua navegação na internet e afins.

Produtos Business (Produtos corporativos)

- ☑ Crie uma senha para seus parâmetros e configuração avançada, isso é essencial para a sua proteção, pois muitas ameaças utilizam dessa "Fragilidade" para atacar o seu sistema e, com uma proteção AV sem senha, a invasão se torna mais fácil.

- ☑ Procure alterar a senha das configurações avançadas com uma frequência de, no máximo, 3 meses. Procure também criar essa senha com letras maiúsculas e minúsculas, além de utilizar, ao menos, um caractere especial.

- ☑ Recomendamos manter sua Base de dados de Assinatura de Vírus sempre atualizada para que as mais recentes ameaças não tenham porta aberta em sua máquina.

- ☑ Agende um rastreamento, no mínimo, semanal no seu produto ESET para ter a certeza de que seu computador estará sempre protegido. Procure programar esse agendamento no próprio produto para não correr o risco de esquecer de realiza-lo.

- ☑ Recomendamos que, em caso de Notebook, no dia agendado para o rastreamento, mantenha o mesmo plugado para carregar a bateria, de forma que não aconteça que a bateria se esgote sem que o rastreamento semanal tenha sido realizado por completo.

- ☑ Procure configurar o Antifurto, nunca se sabe o dia de amanhã.

- ☑ Ao configurar o Antifurto em seu celular (Smartphone) Android procure sempre cadastrar um número confiável. Esse número confiável será utilizado para todos os recursos que você pode obter do recurso "Antifurto" instalado em seu smartphone. Além disso, com esse número confiável você diminui consideravelmente o tempo gasto para proteger seus dados, descobrir a coordenada GPS ou, simplesmente, bloquear e desbloquear o equipamento.

- ☑ No ESET Remote Administrator, adicione a coluna "Usuário Logado" para poder organizar melhor todo o seu ambiente e saber quem está logado em determinada máquina.

- ☑ Procure deixar a senha de Administrador da rede o mais forte possível, pois só ela será capaz de realizar todas as ações possíveis dentro do seu ambiente, isso influencia também na sua segurança, pois só o Administrador poderá alterar as configurações do Antivírus.

- ☑ Procure sempre deixar explícito nas configurações do produto qual conteúdo determinado Usuário terá acesso. Você pode realizar determinada alteração através das políticas no ERA. Dessa forma, você consegue bloquear ou permitir o acesso de determinado (ou todos) usuário à determinado caminho de rede, sites de internet, etc. Isso te protege de que algum funcionário acesse um site perigoso ao qual você já conhece. Você pode bloquear esse site de forma que ninguém possa acessá-lo.

- ☑ Em caso de problemas, utilize a ferramenta ESET SysInspector do seu produto ESET. Essa ferramenta facilita e agiliza muito o atendimento da Equipe de Suporte.

- ☑ Em caso de qualquer dúvida, procure, primeiramente, em nossa Base de Conhecimentos (http://kb.eset.com.br). Muitas vezes a sua solução já foi cadastrada em nossa Base.

- ☑ Verifique sempre a validade de sua licença, a ESET informa com bastante antecedência quando a validade está expirando mas, não se esqueça da mesma, pois ao final dela, você fica totalmente desprotegido.

- ☑ Certifique-se de adicionar os dispositivos portáteis (Pen-drive, HDs Externos, etc) cadastrados no Controle de Dispositivos. Dessa forma, qualquer equipamento que seja plugado em seu ambiente será bloqueado a não ser que esteja cadastrado pelo Administrador no produto. Isso remove uma das portas de ataque de Malware (a porta USB).

- ☑ Se houver algum serviço de firewall de borda ou dispositivo de gerenciamento e redirecionamento de portas, mantenha restrito, com o mínimo possível de portas apontando para os servidores da empresa.

- ☑ Manter o acesso a Terminal Server desabilitado nas estações e, principalmente, servidores.

- ☑ Mantenha o Sistema Operacional sempre atualizado.

Produtos Home (Produtos Residenciais)

- ☑ Caso possua filhos, crie diversas contas de Usuário no Windows de forma a poder proteger com maior eficácia os mesmos através do recurso Controle dos Pais.

- ☑ Crie uma senha para seus parâmetros e configuração avançada, isso é essencial para a sua proteção, pois muitas ameaças utilizam dessa “Fragilidade” para atacar o seu sistema e, com uma proteção AV sem senha, a invasão se torna mais fácil.

- ☑ Procure alterar a senha das configurações avançadas com uma frequência de, no máximo, 3 meses. Procure também criar essa senha com letras maiúsculas e minúsculas, além de utilizar, ao menos, um caractere especial.

- ☑ Recomendamos manter sua Base de dados de Assinatura de Vírus sempre atualizada para que as mais recentes ameaças não tenham porta aberta em sua máquina.

- ☑ Agende um rastreamento, no mínimo, semanal no seu produto ESET para ter a certeza de que seu computador estará sempre protegido. Procure programar esse agendamento no próprio produto para não correr o risco de esquecer de realiza-lo.

- ☑ Recomendamos que, em caso de Notebook, no dia agendado para o rastreamento, mantenha o mesmo plugado para carregar a bateria, de forma que não aconteça que a bateria se esgote sem que o rastreamento semanal tenha sido realizado por completo.

- ☑ Procure configurar o Antifurto, nunca se sabe o dia de amanhã.

- ☑ Ao configurar o Antifurto em seu celular (Smartphone) Android procure sempre cadastrar um número confiável. Esse número confiável será utilizado para todos os recursos que você pode obter do recurso "Antifurto" instalado em seu smartphone. Além disso, com esse número confiável você diminui consideravelmente o tempo gasto para proteger seus dados, descobrir a coordenada GPS ou, simplesmente, bloquear e desbloquear o equipamento.

- ☑ Em caso de problemas, utilize a ferramenta ESET SysInspector do seu produto ESET. Essa ferramenta facilita e agiliza muito o atendimento da Equipe de Suporte.

- ☑ Em caso de qualquer dúvida, procure, primeiramente, em nossa Base de Conhecimentos (http://kb.eset.com.br). Muitas vezes a sua solução já foi cadastrada em nossa Base.

- ☑ Verifique sempre a validade de sua licença, a ESET informa com bastante antecedência quando a validade está expirando mas, não se esqueça da mesma, pois ao final dela, você fica totalmente desprotegido.

- ☑ Mantenha o Sistema Operacional sempre atualizado.

Sobre a NETDEEP TECNOLOGIA:

A NETDEEP TECNOLOGIA está no mercado desde 2009, implementando, indicando e desenvolvendo soluções em Tecnologia e Segurança da Informação. Somos uma equipe multidisciplinar composta por consultores, analistas, programadores, designers, hackers, entre outros especialistas nas tecnologias de ponta mais adequadas para atender a demanda do seu negócio.

Para mais informações visite nosso site: http://www.netdeep.com.br