COMUNICADO PARA OS USUÁRIOS TEF SKYTEF

A Skytef NÃO entra em contato com os clientes usuários do TEF para solicitar acesso remoto ou presencial no ambiente do servidor, do PDV ou do TEF sob nenhum pretexto, incluindo atualizações emergenciais ou rotineiras.

Nunca solicitamos seus códigos de acesso pois são de uso pessoal e intransferível.

Estamos listando a seguir boas práticas de segurança que são necessárias para a segurança do processo de TEF:

1) Oriente sua equipe sobre phishing, normalmente e-mails fakes aonde se solicita que digite sua senha ou chave de acesso. A Skytef nunca envia e-mail pedindo solicitação de senhas.

2) Segmente sua rede. Apesar de não ser um requisito obrigatório, a segmentação reduz o escopo do ambiente e de atuação de um invasor, por isso é altamente recomendada.

3) Antes de implantar a tecnologia Wireless em seu ambiente, avalie esta necessidade contra o risco envolvido. Se precisar implementá-la, utilize os níveis de segurança mais altos possíveis no roteador.

4) Utilize firewall em todos os acessos à rede interna, isto permite a monitoração e o controle, minimizando chances de um indivíduo mal intencionado obter o acesso à rede. Restrinja a divulgação de endereços IPs internos ou privados.

5) Não mantenha senhas e contas (ID) padrões em seus sistemas, mesmo que uma conta padrão não seja utilizada, altere a senha padrão para uma senha exclusiva e se possível desative esta conta.

6) Habilitar nos servidores e PDVs, apenas os serviços necessários ao funcionamento do sistema.

7) Realize periodicamente inventário de hardware e software utilizados em sua rede.

8) Mantenha o Software e o Antivírus sempre atualizados.

9) Restrinja o acesso dos usuários somente aos componentes da rede necessários ao seu trabalho.

10) Atribuir a cada usuário uma conta (ID) exclusiva.

11) Excluir o acesso dos usuários que não tenham mais necessidade de acesso ao sistema ou que não fazem mais parte da equipe. Excluir as contas que fiquem inativas por 90 dias.

12) ID utilizado por fornecedores ou utilizado para acesso remoto deverá ser habilitado somente no momento do uso e desabilitado a seguir.

13) Bloquear a conta quando ocorrer tentativas repetidas e inválidas de acesso de um usuário.

14) Quando ocorrer o bloqueio configure para que a liberação ocorra após um período superior a 30 minutos ou através de habilitação de um Administrador.

15) Exija uma nova autenticação do usuário quando uma sessão estiver ociosa por mais de 15 minutos.

16) Exija que a senha tenha no mínimo 7 caracteres contendo caracteres numéricos e alfabéticos. Estas senhas devem ser alteradas pelo menos uma vez a cada 90 dias.

17) Exigir a troca da senha pelo usuário em seu primeiro acesso.

18) Se o acesso remoto for imprescindível, atente-se à:

a) Incorpore a autenticação de dois fatores. (Senhas, certificados, IPs, etc...);

b) Certifique-se de que ele somente estará habilitado durante o período em que esse acesso for necessário;

c) Certifique-se de quem irá acessar é, de fato, a pessoa que lhe presta esse tipo de serviço;

d) Nunca deixe as senhas de acesso remoto serem a padrão do aplicativo;

e) Utilize aplicativos para acesso remoto que gerem trace e logs do acesso.

19) Restringir o acesso físico ao servidor somente a pessoas autorizadas.

20) Oriente e Treine sua equipe para estarem preparados para detectar e evitar tentativas de adulteração, instalação ou substituição de dispositivos em sua rede.

21) Estabelecer e disseminar uma política de segurança entre sua equipe. Esta política deverá ser revista anualmente e ajustada em função de novas regras de segurança ou aprendizado da própria equipe.

22) Nunca libere o acesso de seu servidor ou de sua rede a pessoas que não sejam conhecidas e autorizadas a ter esse acesso.

23) Em pontos de rede que estejam localizados em ambientes não controlados, como por exemplo na área de vendas, preocupe-se em não deixar que alguém mal intencionado possa utilizá-los para acessar a sua rede interna.

24) Realize diariamente o batimento de vendas de seu PDV com o servidor SiTef.

25) Realize diariamente o batimento de vendas realizadas em seu servidor SiTef com as vendas registradas pelo seu adquirente (extratos).

Aproveitamos também para reforçar mais uma vez que a Skytef não entra em contato com os clientes usuários do SiTef para solicitar acesso, quer seja remoto, quer seja fisicamente no ambiente, com o intuito de fazer atualizações, sejam elas emergenciais, sejam elas rotineiras. As únicas pessoas que podem acessar e atuar no ambiente TEF são as da empresa contratada pelo cliente para esse fim. Sempre confirme que quem está pretendendo ter esse acesso realmente pertence à empresa contratada.

Em caso de dúvidas ou problemas, contate nosso suporte via e-mail suporte.tef@skytef.com.br**, chat online ou pelo telefone (11) 2175-9501.**

Atenciosamente Equipe Suporte TEF