Fortics

CARTILHA DE

# PREVENÇÃO À INVASÃO

## Políticas de Senhas e Direito de Acesso

#JuntosSomosFortics
www.fortics.com.br

**MÓDULOS DE *SOFTWARE* NÃO PERSONALIZADO QUE INTEGRAM A PLATAFORMA FORTICS**

| Produto | Breve Descritivo |
|---|---|
| **FORTICS PBX** | Telefonia Inteligente para a sua empresa lucrar muito mais<br>Leia mais em: http://www.fortics.com.br/fortics-pbx/ |
| **FORTICS PBX (DISCADOR)** | Crie campanhas e aumente a produtividade do seu contact center<br>Leia mais em: http://www.fortics.com.br/fortics-pbx/ |
| **FORTICS SZ.CHAT** | Seu canal profissional de atendimento por redes sociais<br>Leia mais em: http://www.fortics.com.br/fortics-szchat/ |
| **FORTICS ANALYZER** | Auditoria & Análise Avançada de Contas Telefônicas<br>Leia mais em: http://www.fortics.com.br/fortics-analyzer/ |

**INTRODUÇÃO**

Os recursos da PLATAFORMA FORTICS são protegidos por senhas, isso garante acesso somente a pessoas autorizadas.

Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário, etc.

Com relação aos parâmetros para criação da senha de acesso, todo usuário deverá utilizar senha composta de no mínimo 6 dígitos, entre letras (utilizar maiúsculas e minúsculas), números e caracteres especiais que devem ser combinados para maior proteção.

Para maior segurança, limite o acesso a interface de configuração, gerenciamento e facilidades da PLATAFORMA FORTICS e siga as dicas abaixo:

**COMO MANTER UM AMBIENTE SEGURO PARA AS INFORMAÇÕES DA EMPRESA**

- Crie uma política de segurança e passe para todos os usuários, enfatizando a sua importância.
- Utilize mecanismo de controle de acesso remoto, como o código de autorização do PBX.
- Não permita que a configuração do DISA autorize a realização de chamadas sem o uso de senha e procure sempre associar a senha ao ramal físico do usuário, facilitando a identificação da origem das chamadas.
- Restrinja o acesso remoto de operações e manutenção técnica somente a pessoas autorizadas. Compartilhe com elas a responsabilidade de manter em sigilo as senhas do sistema.
- Procure criar senhas de diferentes níveis para identificar, via logs, quem acessou da PLATAFORMA FORTICS.
- Mantenha um backup de dados da PLATAFORMA FORTICS atualizado com o menor intervalo de tempo possível e/ou sempre que houver alteração de algum parâmetro no equipamento.

- Determine restrições de destinos por ramais, conforme o perfil do usuário (local, móvel, DDD e DDI).
- Restrinja a utilização de chamadas tronco-tronco (trata-se de chamadas procedentes de um tronco externo, pedindo autorização para realização de chamada em outro tronco externo).
- Permita o recebimento de chamada a cobrar apenas para ramais estratégicos. Se possível bloqueie esse tipo de chamada para os ramais designados a correio de voz, placa DISA, URA, etc.
- Bloqueie ramais de correio de voz que possam originar chamadas externas.
- Acompanhe os destinos das chamadas nacionais e internacionais, o tempo médio dessas chamadas e as ocorrências de ligações a cobrar, comparando com o perfil histórico dessas chamadas.
- Permita a possibilidade de transferência de chamadas apenas a ramais predefinidos ou à telefonista. Se possível, bloqueie o código de acesso ao tronco externo (“0” ou “9”) em sistemas de atendimento automático (DISA, URA, etc.).
- Seja criterioso para disponibilizar aos funcionários acesso ao correio de voz da empresa, avalie de fato quem precisa dessa facilidade.
- Restrinja a facilidade de call-back externa, liberando-a apenas para ramais de call center.
- Restrinja a conferência entre chamadas, conforme perfil do usuário.
- Impeça a transferência de chamadas recebidas na central de atendimento da empresa (0800) para outros departamentos (ramais) internos.
- Restrinja a facilidade de siga-me externo para os ramais que realmente necessitam.
- Programe a sinalização de desconexão forçada por tempo. Recomenda-se desconectar ligações com duração acima de 2 (duas) horas.
- Utilize redes privadas sem acesso à internet para registro de ramais remotos ou conexão com VoIP.
- Utilize sistemas de controle na administração de servidores de voz, por exemplo, o caso do “SSH” (programa de computador e protocolo de rede que permite a conexão entre computadores, de forma a executar comandos de uma unidade remota) para verificar mensagens ou assegurar os logs. Verifique se não existem tentativas de logon utilizando “bruteforce” ou técnica similar para SIP.
- Utilize redes distintas e separadas para telefonia e para dados, inclusive com a utilização de “Access Point” (dispositivo em uma rede sem fio que realiza a interconexão entre todos os dispositivos móveis) distinto para solução WI-FI. Se possível, separe as redes efetivamente, de forma física, e não apenas utilizando “subnets” (divida uma rede em várias partes, aumentando assim o número de redes e diminuindo o número de hosts) distintas.
- Utilize sistema de provisioning para configurar os ATAs/ramais IPs ativos em rede privada. Caso o ATA/ramal IP esteja exposto na internet, a configuração deve ser individual, evitando a exposição da senha de conta SIP.

- Utilize firewalls, IPS (Intrusion Prevention System), antivírus, antimalwares, restrição de portas na autenticação de ramais, assim como restrição de acesso as configurações dos ATAs e aplique quarentena em endereços IP com números excessivos de tentativa de logon.

- Não exponha os ramais (SIP/IAX/H323) na internet (fixa ou móvel). Se o fizer, procure utilizar tunelamento VPN com autenticação de senha para inibir a exposição do endereçamento IP.

- Mantenha os softwares de seu ambiente computacional sempre atualizados.

- Efetue periodicamente cópias de segurança (backup) e simule periodicamente a validação do processo de restauração das cópias de segurança para garantir a eficácia do procedimento.

**SENHAS DE PROTEÇÃO**

- Alguns elementos que você deve usar na elaboração de suas senhas são: (a) Números aleatórios - quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos. (b) Grande quantidade de caracteres - quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente. (c) Diferentes tipos de caractere - quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequencias alfanuméricas, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

- Utilize uma frase longa que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas à você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "1 dia ainda verei os aneis de Saturno!!!".

- Selecione caracteres de uma frase: “Eu trabalho na FORTICS há 3 anos e 1 mês”: EtnFh3ae1m

- Faça substituições de caracteres, invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha "SS0l, asstrr0-rrei d0 SSisstema SS0larr".

- Troque a senha de todos os recursos (correio de voz, URA, cadeado eletrônico, DISA, etc.) periodicamente, para assegurar um ambiente mais seguro.

- Jamais use o número do ramal como senha do próprio ramal.

- Procure usar senhas até mesmo em ramais de fax e salas de reunião, evitando a invasão interna desses ramais.

- Altere as senhas sempre que ocorrer troca de pessoal responsável da PLATAFORMA FORTICS e demais equipamentos/dispositivos relacionados.

- Modifique as senhas padrão (default) dos ATAs e softphones, mesmo que esses tenham sido fornecidos por provedores VoIP.

- Evite utilizar a mesma senha para acessar diferentes plataformas e/ou dispositivos, isso pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.

- Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.

**POSSÍVEIS CONSEQUÊNCIAS DE UMA INVASÃO**

- Utilização da PLATAFORMA FORTICS para efetuar ligações sem o conhecimento da empresa, gerando faturas com custos elevados.

- Utilização da PLATAFORMA FORTICS para enviar mensagens sem o conhecimento da empresa.

- Destruição, visualização ou acesso a dados confidenciais.

- Criação de “ramais virtuais” (ramais que possuem posição lógica, mas não existem fisicamente) e salas de distribuição de chamadas.

- Risco de paralisação da PLATAFORMA FORTICS, gerando desprogramação e transtornos para a empresa.

- Acesso a PLATAFORMA FORTICS por pessoas não autorizadas que fazem uso de atividades ilícitas, escondendo sua real identidade e localização.

- Modificação de recursos e facilidades da PLATAFORMA FORTICS.

- Criação de salas de conferência na PLATAFORMA FORTICS.

**CONSIDERAÇÕES FINAIS**

Fique atento aos pequenos detalhes. Segurança da informação é muito importante, por isso, faça com que sua empresa utilize os mecanismos de defesa apropriados e siga sempre as melhores práticas de mercado para proteger seu ambiente.

Também recomendamos a leitura da cartilha de marketing por mensageria (boas práticas) disponibilizada pela FORTICS em relação ao uso dos módulos de software não personalizado que integram a PLATAFORMA FORTICS, disponível em http://www.fortics.com.br/pdf/boaspraticasmensageria.pdf.