

# **GUIA DE IMPLEMENTAÇÃO**

## **SiTef 5.0 - PA-DSS 2.0**

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 - Sobreloja H - Cep 01310-300 - PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

Versão 1.5      Pag. 1

## Índice

1. SiTef.....	3
2. PCI / AIS .....	4
3. Armazenamento de Dados do Cliente.....	6
4. Transmissão de dados do Cliente por e-mail. ....	7
5. Rede Segura. ....	8
6. Backups. ....	11
7. Comunicação Client/Servidor/Autorizador.....	11
8. Controle de Vulnerabilidade. ....	12
9. Monitoração do Servidor. ....	13
10. Teste de Segurança. ....	14
11. O servidor SiTef e o PDV .....	15
12. Plano de resposta a incidentes .....	18
13. Política de Segurança. ....	18
14. Check List. ....	19
15. Atualização dos módulos. ....	21
16. Acesso remoto ao servidor SiTef para manutenção .....	21
17. Anexo A - Desabilitando Serviços Desnecessários.....	23
18. Anexo B - Atualizações e Patches de Segurança .....	26
19. Anexo C – Solicitação de alteração de ambiente .....	28
20. Anexo D - Configuração do Sistema operacional Windows para logon/auditoria.....	31
21. Anexo E - Sincronização de horário no servidor Windows 2000, XP e 2003 .....	36
22. Anexo F – Configurando Exportação de Log do Sistema .....	37
23. Mantendo políticas perante Clientes e Integradores .....	38
24. Histórico de alterações.....	38
25. Glossário .....	39

## 1. SiTef

O **SiTef** é responsável pela formatação das mensagens e a comunicação com as Redes Adquirentes (*Redes Autorizadoras*) competentes. As Redes Adquirentes, por sua vez, são responsáveis pelo processo de autorização das transações.

O **SiTef** é uma interface utilizada para conectar Terminais requisitantes de operações de transferência eletrônica de fundos com as administradoras responsáveis por esta transferência.

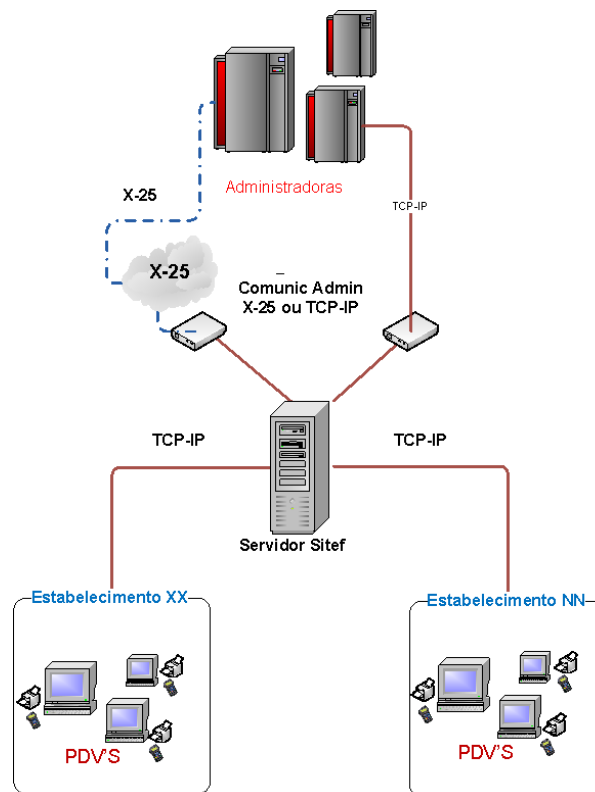
A execução de uma transação TEF exige uma série de informações, conforme especificações técnicas de cada administradora (Adquirente), que são geradas tanto no próprio **SiTef**, em função de padrões e configurações adotadas, como provenientes dos Terminais.

O **SiTef** foi desenvolvido de modo que, a quantidade de informações exigidas dos Terminais fosse a menor possível, visando simplificar a operação e o desenvolvimento do mesmo.

Entende-se por Terminal, um PDV (Ponto de Venda ou check-out) de um estabelecimento comercial, ou um software aplicativo que possibilite a captura de dados de uma transação financeira ou de uma consulta a cheques, que envolva uma transferência eletrônica de fundos, ou de uma consulta a documentos, gerando assim débitos e créditos em contas correntes em questão (do cliente e do lojista).

É responsabilidade do Terminal coletar os dados das transações, exibir a resposta e imprimir o cupom TEF.

Para o Terminal a Software Express disponibiliza os módulos CliSiTef ou ClientSiTef Modular que são escolhidos dependendo do compilador utilizado pela Automação Comercial e/ou do sistema operacional utilizado no PDV.



Ao utilizarmos o protocolo **TCP/IP** para comunicação junto as Redes Adquirentes, podemos nos deparar com as seguintes possibilidades:

- ✓ Link TCP ponto a ponto: Neste caso, recomenda-se criar uma VPN/IPSec com criptografia;
- ✓ Link TCP ponto a ponto (MPLS): Neste caso, recomenda-se criar uma VPN/IPSec com criptografia, desabilitando o acesso à internet (configuração por parte da operadora);
- ✓ Link TCP via internet (redes públicas): Obrigatoriamente, criar uma VPN/IPSec e, utilizar algoritmos de criptografias e chaves aceitas pelo PCI-DSS (normas vigentes);

## 2. PCI / AIS

### O que é PCI?

O PCI não é uma lei federal, como HIPAA, SOX e GLBA, mas sim um padrão privado de segurança, que estabelece como administradores e operadores de terminais de cartões de pagamento e prestadores de serviços devem proceder ao firmar contratos com companhias de cartões de crédito, como Visa, MasterCard, American Express, etc.

### O que é AIS?

É um Programa de Segurança da Informação (A/S) introduzido na **Cielo** para a América Latina e Caribe no ano de 2000. Ele estabelece que todos os Membros (Emissores ou Adquirentes), Agentes, Estabelecimentos e Prestadores de Serviços que armazenam,

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobreloja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

processam ou transmitem a informação e as transações dos Portadores de Cartão devam cumprir com as Normas de Segurança da Informação.

Os padrões do PCI-DSS oferecidos no AIS foram desenhados para proteger a confidencialidade, disponibilidade e integridade dos dados do portador de cartão.

### **Quem está sob as regras do PCI?**

O PCI se aplica a todos os administradores de cartões de pagamento, estabelecimentos comerciais e prestadores de serviços que processam ou transmitem dados de usuários de cartões, independentemente se o dado é recebido em um ponto de venda, por telefone, através de comércio eletrônico ou por qualquer outro modo de transação. O PCI-DSS se aplica a todos os componentes do sistema, incluindo componente de rede, servidor, ou qualquer aplicativo incluído ou conectado ao ambiente de acesso às informações do portador do cartão.

Os requisitos de segurança se aplicam a todos os “*componentes do sistema*”. Os componentes do sistema são definidos como qualquer componente servidor, ou aplicação da rede, incluído ou conectado ao ambiente de dados do portador do cartão. A segmentação adequada da rede, que separa os sistemas que armazenam, processam ou transmitem os dados do portador do cartão daqueles que não o fazem, pode reduzir a extensão do ambiente dos dados do portador do cartão. (Firewalls, switches, routers, etc).

O padrão do PCI-DSS é dividido em seis categorias, tendo sempre como intuito proteger números de cartões de crédito e outros dados importantes dos usuários.

### **Categoria 1: Construa e mantenha uma rede segura**

1. Instale e mantenha uma configuração de firewall para proteger os dados;
2. Não utilize as senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços;

### **Categoria 2: Proteja Dados do Portador de Cartão**

3. Proteja dados armazenados;
4. Codifique a transmissão dos dados do portador de cartão e as informações importantes que transitam nas redes públicas;

### **Categoria 3: Mantenha um programa de controle de vulnerabilidade.**

5. Use e atualize regularmente o software antivírus;
6. Desenvolva e mantenha seguros os sistemas e aplicativos;

#### **Categoria 4: Implemente rígidos controles de acesso**

7. Restrinja o acesso aos dados para apenas aqueles que necessitam conhecê-los para a execução dos trabalhos;
8. Atribua um ID único para cada pessoa que possua acesso ao computador;
9. Restrinja ao máximo o acesso físico aos dados do portador de cartão;

#### **Categoria 5: Regularmente monitore e teste as redes**

10. Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão;
11. Teste regularmente os sistemas e os processos de segurança;

#### **Categoria 6: Mantenha informação de uma política de segurança**

12. Mantenha uma política que atenda à segurança da informação.

Outras informações sobre o PCI poderão ser obtidas no site <https://www.pcisecuritystandards.org/>. Referência sobre o tema também poderá ser obtida através das normas ABNT do grupo 27000.

### **3. Armazenamento de Dados do Cliente**

O SiTef esta desenvolvido de forma a disponibilizar aos seus usuários apenas os dados permitidos. Em alguns casos específicos o número do cartão é disponibilizado, outros dados como tarja magnética e código de segurança (CVC2, CVV2, CI) não devem ser armazenados. Tabela - Armazenagem dos dados *permitida/não permitida*:

	Elemento do Dado	Armazenagem Permitida	Proteção Exigida	PCI DSS Req. 3.4
Dado do Portador de Cartão	Número Primário da Conta (PAN)	SIM	SIM	SIM
	Nome do Portador do Cartão	SIM	SIM	NÃO
	Código do Serviço	SIM	SIM	NÃO
	Data de Vencimento	SIM	SIM	NÃO
Dados Confidenciais de Autenticação	Tarja Magnética Completa	NÃO	NÃO	N/A
	CVC2/CVV2/CI	NÃO	NÃO	N/A
	PIN / Bloqueador de PIN	NÃO	NÃO	N/A

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

onde:

**PAN** (*Primary Account Number*) - é o número do cartão;

**PIN** (*Personal Identification Number*) - é uma senha numérica secreta compartilhada entre o usuário e um sistema;

**Bloqueador de PIN** - é uma senha numérica secreta *criptografada* compartilhada entre o usuário e um sistema;

a. **O SiTef não efetua armazenamento de cartões**, mas como existem clientes que podem utilizar uma modalidade de transação chamada “*Recorrente*”; (por exemplo, assinatura de revistas, jornais,...etc) recomendamos que esses dados sejam protegidos utilizando-se chaves de criptografias, como Triple-DES 168-bit (*tripla chave*) ou AES 256-bit, associada com os processos e procedimentos de administração de chave.

b. Recomendações quanto à exibição dos dados:

- i. Nunca armazenar o código de segurança ou valor de validação do cartão;
- ii. Ocultar parcialmente o PAN do cartão (número do cartão) ao exibi-lo em tela. Exibir conforme especificação das autorizadoras (6 primeiros e 4 últimos);
- iii. Torne o PAN ilegível em qualquer local em que seja necessário armazená-lo.
- iv. Nunca armazene o PIN do cartão;
- v. Codificar informações pessoais; *Utilizando chaves de criptografias como por exemplo o como TDES 168-bit (tripla chave) ou AES 256-bit associada com os processos e procedimentos de administração de chave*

#### **4. Transmissão de dados do Cliente por e-mail.**

O SiTef não armazena em seus arquivos de auditoria (\SiTef\Audit) dados de cartão, apenas o PAN do cartão (utilizando criptografia AES-128 bits, recomendada pelo PCI) em arquivos de LOG (SiTef\Log), de modo temporário, devido às especificações de algumas adquirentes, e por causa de transações pendentes que ainda poderão ser desfeitas. Sendo assim, quando necessário acionar o suporte da Software Express, e lhe forem solicitados tais arquivos, os mesmos poderão ser enviados qualquer sem problema ou comprometimento da segurança.

Porém, é importante salientar que **nunca** se deve enviar o PAN não codificado por e-mail. Caso necessário este envio, o procedimento é gravar esta informação em um arquivo texto,

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

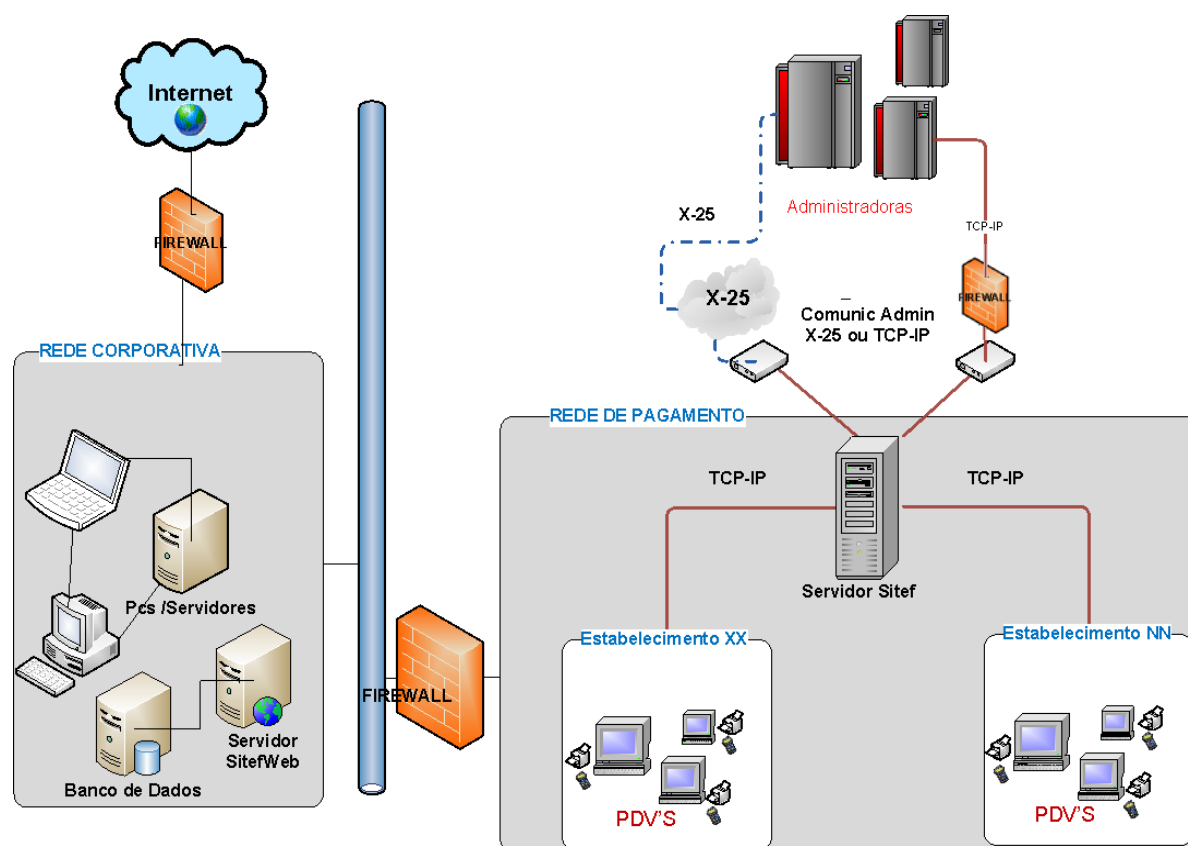


compactar este arquivo com senha (utilizando algoritmos de criptografia forte) e enviá-lo em um e-mail com senha de abertura, que será enviada ainda, em um segundo e-mail (ambos com de *criptografia forte*, ou outras tecnologias de mensagem de usuário final).

## 5. Rede Segura.

Segmentação de ambiente TEF (Construa uma rede segura. Todos os sistemas devem ser protegidos contra acesso não autorizado).

Utilize Firewalls, Switches, Routers, pontos de acesso, Wireless e aplicações de rede para restrição ao ambiente TEF, Exemplo a Topologia abaixo:



Criar uma “Rede de Pagamentos”, onde a mesma esteja isolada (segmentada) das demais redes. No desenho anterior foi apresentada uma estrutura onde o servidor SiTef se encontra isolado (da internet e de outras redes) pela inclusão de um firewall na topologia padrão.

1. Rede Segura (Mantenha uma rede segura), Hackers (externos ou internos) geralmente utilizam as senhas padrões dos prestadores de serviços e outros parâmetros padrões para comprometer os sistemas.

- a. Troque sempre os padrões de senha estabelecidos antes da instalação de um sistema na rede. Desenvolva um padrão que atenda todas as vulnerabilidades de segurança conhecidas. Recomenda-se associar requisitos mínimos de complexidade de senha com requisitos de força

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizada previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*



(esforço/dificuldade para quebra da senha) em um só, e aumentar a flexibilidade nessas alternativas (Requisitos mínimos: Controle de acesso, ID de usuário único no sistema, e autenticação segura);

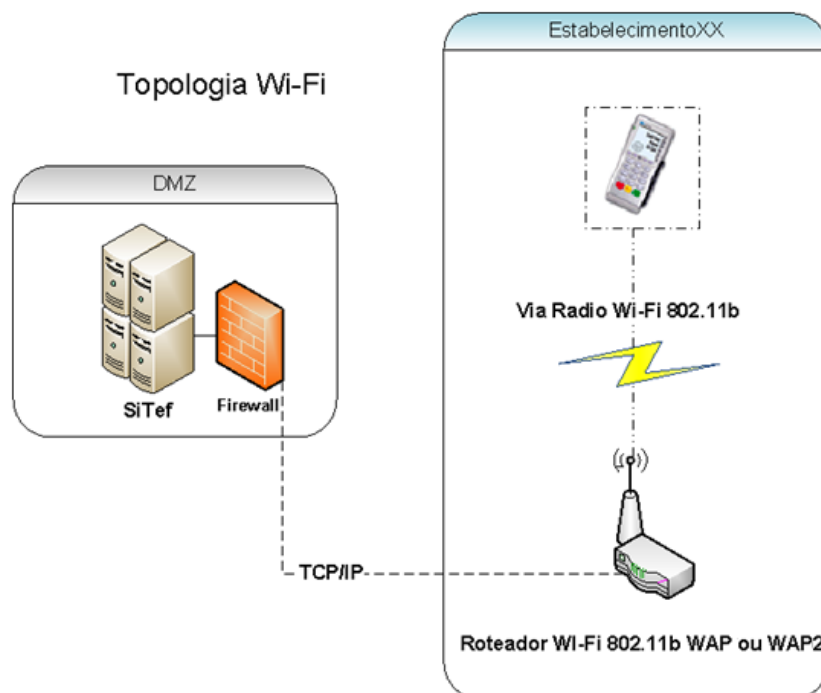
- b. Crie política de senhas. Utilize mínimo 7 caracteres, com letras, números e caracteres especiais;
- c. Desativar serviços e protocolos inseguros, bem como funcionalidades não utilizadas (*Vide Anexo A*);
- d. Codifique todo acesso administrativo que não seja via teclado; Exemplo: Use tecnologias tais como SSH versão 2, VPN (utilizando algoritmo de criptografia T-DES 168 bits, AES-128 bits), ou SSL/TLS v.3 / TLS v.1 para a administração baseada na web e outro acesso administrativo via unidade de teclado.
- e. Manter patches de segurança atualizados (em até 1 mês após o lançamento). Habilitar criptografia ALTA para o protocolo RDP, utilizado pelo aplicativo “Conexão de área de trabalho remota”;
- f. Implementar processos para identificar vulnerabilidades de segurança;
- g. Implementar documentos para controle de mudanças (Descrição da mudança, criticidade, aprovações internas, liberação de acesso, documento de impacto, procedimentos de *Rollback* etc - *Vide Anexo B e C*);
- h. Aprimorar exigências para inclusão de mudanças relativas à identificação e mecanismos de autenticação (criação de novas contas, alteração/aumento de privilégios/poderes dentro do sistema operacional), bem como outras mudanças como, adições/exclusões de contas com raiz ou acesso administrativo.
- i. Restringir o acesso aos dados do portador do cartão
- j. Restringir o acesso de terceiros ao ambiente TEF (Limitação de acesso);
- k. Criar ID único para cada usuário, inclusive para acessos remotos. (Proibido senhas compartilhadas).

2. Caso exista rede Wireless, deverão ser instalados *Firewalls* nos perímetros desta rede para que a mesma fique isolada, bloqueando o acesso à *Rede de Pagamento*. Caso a rede Wireless seja utilizada para objeto do negócio (pela rede corporativa da empresa), utilizar também outros *Firewalls* para controlar estes acessos.

- a. Configurações **default** (*padrão de fábrica*) do dispositivo wireless devem ser alteradas:
  - i. Chaves de criptografia;
  - ii. Default **SNMP Community String** (*vide glossário*)

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

- iii. Padrões de senhas;
  - iv. Firmware dos dispositivos sem fio, a fim de proporcionar maior robustez na criptografia;
  - v. Outros valores **default** de padrões de segurança do fabricante (se aplicável).
- b. Em ambiente Wireless altere os padrões do prestador de serviço, incluído chaves WEP, padrão SSID, senhas, e **SNMP community string** e desativação de transmissão de SSID. Caso o ambiente permita, habilite a WPA (Wi-Fi Protected Access) para a codificação e autenticação.
- c. Cifrar (**vide glossário**) com tecnologias WPA ou WPA2, VPN IPSEC ou SSL/TLS as transmissões para rede sem fios que trafegam dados do portador do cartão. Caso estejam sendo utilizadas implementações WEP, as mesmas devem ser migradas para WPA ou WPA2.
- i. Usar somente em conjunto com tecnologias WPA e WPA2, VPN ou SSL/TLS;
  - ii. Trocar as chaves compartilhadas trimestralmente ou automaticamente se a tecnologia permitir;
  - iii. Trocar as chaves compartilhadas sempre que existirem mudanças de pessoas com acesso a elas;
  - iv. Restringir o acesso baseado em endereços MAC.



- v. Aprimorar exigências para inclusão em inventário de pontos *wireless* de acesso autorizado, bem como uma justificativa comercial (um documento formal) para auxílio na varredura de dispositivos *wireless* não autorizado. Inclusão de novo requisito (plano de incidentes/responsabilidade) afim de aprimorar procedimentos de teste já existentes, e procedimentos de resposta a incidentes, caso novos pontos de acesso sem fio forem detectados.

## **6. Backups.**

Embora o PAN do cartão seja armazenado no SiTef apenas para algumas adquirentes, e de modo temporário (\Sitef\Log) conforme descrito no **item 4** deste documento, o backup dos arquivos de configuração do mesmo são altamente recomendados. Já o backup de informações relativas às transações, viabiliza apenas, um histórico financeiro para o estabelecimento comercial.

- a. O backup deverá possuir identificação.
- b. Para dados do portador do cartão, incluir ainda uma identificação de confidencial.
- c. As mídias podem ser destruídas cortando em sentido cruzado com picotador de papel ou incinere ou reduza à polpa de materiais de cópia física. (ou ainda neutralize com campo magnético do processo de degauss). Os dados não podem ser reconstituídos.
- d. Inventário rigoroso de todas as mídias, bem como, a armazenagem de forma segura.
- e. Armazenar em local segura de preferência fora das instalações;
- f. Manter controle rigoroso sobre qualquer distribuição interna ou externa de qualquer tipo de mídia;
- g. Obter autorização da administração para o transporte das mídias, quando transportadas fora da área de segurança;
- h. Manter inventário rigoroso de todas as mídias.

## **7. Comunicação Client/Servidor/Autorizador.**

Com relação aos protocolos utilizados normalmente temos que, para transações via protocolo X.25, o tráfego de informações ocorre em uma rede considerada privada, pois no mercado Brasileiro, o link X.25 (link dedicado contratado) não possui saída para Internet. Já

no caso do protocolo TCP/IP deve-se considerar proteger esta comunicação (por exemplo, utilizando criptografia SSL v.3 e VPN/IPSEC usando algoritmos de *criptografia forte*).

A comunicação entre os Clients (PDVs) e o servidor SiTef ocorre pelo protocolo TCP/IP (com criptografia TDES-168 bit - tripla chave), caso esta comunicação esteja sendo realizada em uma rede aberta, internet, Wifi, GSM ou GPRS utilizar conexões seguras (SSL v.3) e VPN/IPSEC.

## **8. Controle de Vulnerabilidade.**

- a. Restrição de acesso físico ao servidor. Mantenha controle de acesso (Autorização e identificação física) para registro de evidência. Manter registros por no mínimo 3 meses e a destinação dos privilégios aos indivíduos seja baseada na classificação do trabalho e função, a exigência de um formulário de autorização assinado pela administração que especifique os privilégios solicitados, a existência de um controle de acesso automatizado ou utilização de um Datacenter seguro ou onde possua os recursos de segurança físico, como identificação, autorização de entrada, câmeras, segurança
- b. Efetuar controle de acesso físico a áreas contendo dados sensíveis mesmo entre os próprios funcionários, incluindo um processo para autorizar o acesso, e revoga-lo imediatamente após rescisão contratual;
- c. Rastreabilidade de todos os acessos; Ter controle e utilizar meios para identificar todos os acessos as lojas e matriz. Controle de alteração de software e hardware de todos os equipamentos de TEF, arquivando estes acessos para ter um histórico de todas as pessoas que acessam e acessaram o ambiente TEF.(Como histórico da troca de PinPad, Troca de impressora, troca de caixa, manutenção e atualização de equipamentos, acesso a sala do servidor, acesso ao software de PDV.)
- d. Implementar Anti-Virus e baixa automática de lista (atualização) para proteção contra vírus, Spyware e Adware. O antivírus não pode ser desativado ou alterado por usuários (sem permissões/atribuições para tal), á menos que, especificamente autorizados pela Gerencia (a atribuição dessas permissões deve ser analisada caso a caso).
- e. Avaliar a evolução das ameaças de *malware* para quaisquer sistemas que não sejam considerados usualmente/comumente afetados (anualmente);
- f. Assegurar que todos os aplicativos que funcionam por meio de Web estejam protegidos contra ataques conhecidos; Exemplo: Verifique se a instalação principal do software de antivírus está habilitada com *updates* automáticos e *scans* periódicos.

- g. Locais onde outros mecanismos de autenticação são utilizados (por exemplo: *tokens* de segurança físicos ou lógicos, cartões inteligentes, certificados); os mesmos devem ser vinculados a uma conta individual garantindo que apenas um determinado usuário terá acesso ao local;
- h. Proteger dispositivos que interagem fisicamente e capturam dados de pagamento de cartão (exemplo: *PinPad* e leitores em geral) através da interação física direta contra adulteração e substituição dos mesmos. As empresas devem inspecionar periodicamente seus dispositivos para avaliar e detectar possíveis adulterações (exemplo: *Skimmers*, são dispositivos físicos colocados em cima dos originais para coleta de dados) ou substituição (troca não autorizada por dispositivo modificado e fraudulento).

## 9. Monitoração do Servidor.

Monitoração de acesso (Acompanhe e monitore todo acesso aos recursos de rede e dados do portador do cartão)

- a. Implementar registros de auditoria automatizados em todos os componentes do sistema para reconstrução dos seguintes eventos
  - i. Acesso de qualquer usuário
  - ii. Qualquer ação tomada por usuário com perfil de *root* ou administrador
  - iii. Acesso a todos os registros de auditoria
  - iv. Tentativas de acesso lógico inválidas
  - v. Uso de mecanismos de identificação e autenticação
  - vi. Inicialização dos logs de auditoria
  - vii. Criação ou eliminação de objetos ao nível de sistemaExemplo: Habilitando a auditoria logon/logoff, habilitando, Alerta de eventos, Também havendo a possibilidade de utilizar um servidor de logs como exemplo o software de controle Syslog.
- b. Gravar pelo menos os seguintes registros de auditoria
  - i. Identificação do usuário
  - ii. Tipo de evento
  - iii. Data e Hora
  - iv. Indicação de sucesso ou falha
  - v. Origem do evento
  - vi. Identidade ou nome do dado, componente do sistema ou recurso afetado
- c. Revisar periodicamente os logs de todos os componentes do sistema;
- d. Sincronizar os relógios e datas de todos os sistemas críticos;

- e. Fazer backup dos *registros de segurança* e mantê-los por pelo menos 90 dias. Os exemplos abaixo desta funcionalidade podem incluir, mas não estão limitados a:
- Armazenar os LOGs do Sistema através de *mecanismos de arquivos (padrão da indústria)*, tais como Sistema de Registro Comum de Arquivos (IFT), Syslog, Texto Delimitado, etc; (Vide **Anexo F**, documento que descreve configuração necessária para habilitar aplicativo SysLog)
- f. O processo de monitoração do servidor poderá ser realizado de forma remota desde que a comunicação entre a estação de trabalho e o servidor seja realizada através de uma conexão segura SSL/IPSEC.

## 10. Teste de Segurança.

- a. Efetuar *scan* de vulnerabilidades periodicamente. Exemplos de alguns Software disponíveis para efetuar Scan, NetBrute Scanner download, Symantec Security Check download, LANguard Network Scanner download, Infiltrator Network Security Scanner download
- b. Efetuar testes de penetração contratando empresas especializadas e/ou implementar uma metodologia para os mesmos. Se o nó (segmentação) estiver sendo usada para isolar o ambiente que contém os dados do titular do cartão, de outras redes; devem-se realizar testes de penetração (uma abordagem) para validar se os métodos de segmentação são operacionais e eficientes. Esta abordagem deve ser aceita pela indústria de cartão, o que significa cobrir todo o perímetro e sistemas críticos do ambiente que contenha os dados do titular do cartão, incluir testes de dentro (para fora) e de fora (para dentro) da rede que abranja: Camada de rede (*network-layer*), vulnerabilidades da camada de aplicação (*application-layer*), bem como levar em consideração as ameaças e vulnerabilidades que apareceram nos últimos 12 meses.
- c. Incluir sistemas de detecção de intrusão; Existem vários software disponíveis conhecidos como IDS.
- d. Incluir software para validar a integridade de arquivos a softwares disponíveis para esta validação.
- e. Realizar uma **avaliação de risco**, pelo menos, anualmente e após alterações significativas no meio ambiente.



## 11. O servidor SiTef e o PDV

O SiTef deverá ser instalado em um equipamento exclusivo. Neste servidor o acesso à internet também deverá estar bloqueado, sendo possível de liberação somente nos momentos de atualização dos *paths do sistema* operacional ou antivírus.

São compatíveis os seguintes sistemas operacionais: Windows Server 2003, 2008 e 2012 (recomendamos que sejam utilizadas apenas versões que possuam suporte de segurança da Microsoft).

O mesmo se aplica ao PDV, o equipamento deve estar isolado da Internet, ocorrendo regularmente atualizações de anti-vírus e paths do sistema operacional.

No PDV e no servidor SiTef, além da conta com privilégios de administrador (sempre utilizando ID único), devem ser criadas outras contas de usuários (sem privilégios administrativos) que, obrigatoriamente, efetuem tarefas de rotina ou necessitem de acesso para manutenção. Os privilégios de administrador devem ser delegados somente a pessoas que realmente necessitem e, mesmo assim, através de contas específicas.

No servidor SiTef, tendo em vista que nem todo usuário do Windows pode ter acesso aos módulos do SiTef, será obrigatória a criação de dois grupos de usuários, "SiTef-Adm" e "SiTef-Rel", e apenas os usuários que pertençam a esses grupos poderão acessar, respectivamente, os configuradores e relatórios. Os utilitários assumem o usuário corrente e irão confrontá-lo com o cadastro do Windows para autorizar ou não a execução do aplicativo.

O anti-vírus deve ser instalado no servidor SiTef, porém para melhoria de performance, sugerimos a criação de filtros eliminando a varredura dos diretórios e subdiretórios da árvore SiTef, exceção feita ao diretório "\\SiTef\\plic.win", que deverá ser verificado.

Para a monitoração da tela do SiTef a partir de sua versão, "4.0", está disponível o aplicativo "\\SiTef\\APLIC.WIN\\ ControleGeralSitef.exe", para todos os usuários, porém somente um usuário pertencente ao grupo "SiTef-Adm" poderá finalizar um aplicativos. Veja figura abaixo:





O período de retenção dos arquivos de LOG (SiTef\Log\LOG\_MMDD.DAT) e arquivos de AUDIT (SiTef\Audit\MMDDhhmm.XXX) no SiTef são de 45 dias. Após esta data, o expurgo destes dados ocorre de forma automática.

,onde:

MM=mês;

DD=Dia;

hh=hora;

mm=minuto;

XXX = extensão adotada para cada Adquirente (**051** = Banrisul, **003**=Amex, **181**=GetNetLac, etc).

O SiTef não possui requisitos de banco de dados ou componentes adicionais de Sistema Operacional. Valem algumas recomendações:

Requisitos mínimos de hardware:

- Microcomputador com S.O Windows compatível;
- 1 Gbyte de memória RAM;
- Disco rígido de 80 GB;
- Periféricos: Teclado e Mouse, Monitor VGA, unidade de CD ou USB e placa de rede compatível com protocolo utilizado (TCP/IP);

Indicamos Serviços necessários:

- SiTef- Solução Inteligente para TEF
  - Serviços de perfil de usuário
  - Serviços de Redes (Protocolo TCP/IP, Logon de rede, etc).
  - Horário do Windows
- (bem como, serviços essenciais do sistema operacional em questão).

Porta utilizada na comunicação entre **SiTef-PDV-SiTef**: 4096

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

Porta utilizada na comunicação entre **SiTef-Adquirentes**: Não existe um padrão definido, estas portas são acordadas com cada a área de infraestrutura de cada rede adquirentes.

Porta de comunicação entre **Server SiTef-Server System Logs**: Os logs de sistema são exportados para um outro servidor via protocolo UDP porta **514**.

## Chaves internas de criptografia

O SiTef possui algumas chaves internas de criptografia utilizadas para proteção dos dados dos portadores de cartão durante o processo de autorização de uma transação (estas chaves não são distribuídas). Segundo as regras do PCI e PA-DSS essas chaves **devem ser trocadas anualmente**. Na versão atual do SiTef elas ainda não são trocadas anualmente de forma automatizada. Sendo assim, cabe ao responsável pelo estabelecimento o acionamento da nova versão de chaves na tela de Controle Geral do SiTef, afim de forçar esta troca. Para isto, acionar o botão “Segurança” existente na parte superior do controle geral do SiTef. Neste momento, uma pergunta de confirmação será exibida e as chaves serão trocadas automaticamente pelo SiTef.

Note que a troca deve ser feita em momento que o SiTef não está processando transações uma vez que as transações em vôo poderão ser perdidas caso a troca ocorra entre a resposta do SiTef ao PDV e o recebimento da confirmação da transação ou caso existam transações off-line para serem transmitidas.

A mesma função disponibilizada para troca anual das chaves pode ser acionada para uma troca forçada em período menor caso exista a suspeita de violação da mesma.

Em ambas as situações, entrar em contato com a Software Express para saber como proceder de forma que o *risco de perda* de informações seja minimizado.

Esta chave é gerada de modo randômico dentro do SiTef e não existe digitação de chaves por parte do usuário. Ao solicitar uma nova chave, o SiTef zera as chaves anteriores (sobrescrevendo-as de modo seguro) e cria uma nova chave (Este processo de troca de chaves é absolutamente necessário pelo PCI-DSS). Caso ocorra alteração no arquivo onde as chaves estão gravadas (intervenção manual), as transações ainda persistem com a chave original, pois a mesma se encontra carregada em memória. Já em um segundo momento, após a finalização e inicialização do serviço do SiTef, o arquivo é sobrescrito pelo concentrador SiTef com as chaves originais (geradas pelo algoritmo de criptografia do SiTef).

Com relação ao gerenciamento das chaves:

- ✓ Como o SiTef gera automaticamente essas chaves, e sem qualquer intervenção humana, *algoritmos fortes* já fazem parte de seus requisitos de segurança;
- ✓ Nenhum usuário possui acesso às chaves;

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

- ✓ As chaves (modo criptografado) estão localizadas em: \SiTef \ETC\<nome da rede.bin> (uma chave gerada por rede);
- ✓ Solicitar a troca das chaves anualmente conforme descrito acima.

## **12. Plano de resposta a incidentes**

- a. Crie e implemente um plano de resposta a incidentes. Este plano deve orientar aos operadores os processos a serem realizados no momento de identificação de um incidente. Por exemplo, quem deve ser acionado caso ocorra queda de comunicação do um servidor;
- b. Teste o plano uma vez por ano;
- c. Designe funcionário 24x7 para responder a alertas;
- d. Faça treinamento apropriado;
- e. Incluir alertas originários de detecção de uma intrusão, penetração de sistema;
- f. Crie processo para identificar e desenvolver um plano de resposta a um incidente; Assegure-se de que o plano atende, pelo menos, aos procedimentos de resposta específicos, processos de recuperação de negócios e continuidade, processos de backup dos dados, desempenho e responsabilidades e estratégias de comunicação e contatos (por exemplo, informar as Adquirentes e associações de cartões de crédito), procedimento de *Rollback*, migração de servidor, etc.
- g. Implemente um processo para responder a quaisquer alertas gerados por mecanismos de detecção de mudança (Exemplo: Substituição de programas/executáveis, etc.);
- h. Pode-se efetuar uma replicação dos dados de um servidor de aplicação para outro servidor *Stand Alone* de modo *on-line*.

## **13. Política de Segurança.**

- a. Divulgue, mantenha e dissemine políticas de segurança para todos os funcionários; Exemplo: disponibilizando documentos, colando cartazes, palestras, reuniões e treinamento de clientes e todos envolvidos com a empresa.

- b. Inclua um programa formação de conscientização da segurança na empresa; Exemplo: informativos, Folhetos, circulares e e-mails com as normas de segurança.
- c. Desenvolva políticas definindo o uso por funcionários que lidam com tecnologias críticas. Exemplo: Termos de responsabilidade, documentos que expliquem as normas e procedimentos de segurança.

## 14. Check List.

Para que o ambiente TEF esteja de acordo com as normas PCI deve-se então validar os seguintes pontos:

1. Ter instalada a versão **5.0** ou superior do SiTef.
2. Validar requisitos mínimos de hardware;
3. Desativar todos os serviços e protocolos inseguros e desnecessários (vide **anexo A**). São serviços e protocolos não diretamente necessários para execução do processo;
4. Habilitar os serviços necessários para execução do programa SiTef (**Item 11**);
5. Liberar a porta 4096 para comunicação entre **PDV/SiTef/PDV** (firewall);
6. Liberar portas específicas acordadas com as redes adquirentes para comunicação entre **SiTef/Adquirentes** (caso o protocolo TCP/IP seja utilizado);
7. Ter todos os arquivos de versões anteriores eliminados. Para se remover arquivos de disco deve-se primeiro gravar nestes arquivos dados inválidos e depois removê-los;

**Obs.:** Com relação aos arquivos armazenados dentro do servidor SiTef, o mesmo os armazena por 45 dias seus logs, e mesmo não armazenando qualquer tipo de dados sensíveis, expurga os mesmos automaticamente depois deste período (Tal remoção é absolutamente necessária para estar em conformidade com o PCI-DSS);

8. Caso o estabelecimento (lojista) tenha algum acordo (liberação) com as redes adquirentes para armazenamento de informações confidenciais ou dados, as mesmas também devem ser removidas periodicamente e seu processo de remoção deve ser estabelecido em dois passos, primeiro a gravação de dados inválidos e depois a remoção;
9. Nos casos em que seja necessária a coleta de informações para a solução de um problema, estes dados deverão ser armazenados de modo criptografado em um local específico/conhecido e de acesso limitado. Salientamos que, deve-se apenas coletar a quantidade necessária para resolver um problema específico. Com relação a sua

remoção, também deve-se seguir os processos de segurança descritos em itens anteriores (apagá-los com segurança, e imediatamente após o uso). Exemplo: Compactar arquivo com senha, utilizar softwares de criptografia, remoção de dados, etc;

10. Nos casos em que os dados do portador são armazenados, este armazenamento nunca poderá ser realizado em equipamentos acessíveis pela internet, por exemplo, um servidor Web e servidor de dados na mesma máquina;

11. Tanto o servidor SiTef quanto os PDVs deverão ser acessados:

- a. Por contas com IDs exclusivos, e com direito de administrador somente em casos específicos. Caso este usuário não acesse mais esta máquina, sua conta deverá ser eliminada (Não solicitar ou usar qualquer grupo compartilhado ou contas genérica/senhas);
- b. Empregar pelo menos um dos métodos a seguir para autenticar todos os usuários:
  - ✓ Algo que você sabe, como uma senha ou frase secreta;
  - ✓ Algo o que você tem, como um dispositivo de token ou cartão inteligente;
  - ✓ Algo que você é, como por exemplo, uma biométrica;
- c. Estas contas também deverão ter a senhas criadas com no mínimo 7 caracteres contendo letras e números e caracteres especiais;
- d. As senhas deverão ser trocadas no máximo a cada 90 dias;
- e. Manter histórico de senhas e solicitar que uma nova senha seja diferente das 4 senhas anteriores. Recomenda-se associar requisitos mínimos de complexidade de senha com requisitos de força (esforço/dificuldade para quebra da senha) em um só, e aumentar a flexibilidade nessas alternativas;
- f. Uma sessão deverá ser bloqueada caso fique inativa por mais de 15 minutos (o aplicativo deve exigir que o usuário se autentique novamente para reativar a sessão);
- g. Implementar numero limite de repetidas tentativas de acesso, e bloquear a conta do usuário após não mais de 6 tentativas de *logon*;
- h. Definir uma duração de bloqueio por acesso incorreto da conta (mínimo de 30 minutos ou até que o administrador reative o ID de usuário);
- i. Atribuir autenticação segura para todas as contas padrão (mesmo que não forem ser utilizadas) e, em seguida, desativar ou não utilizar essas contas.

**Obs.:** Conforme descrito em documento anexo (**Anexo D**).



12. Para a rede de pagamentos deve-se implementar registros de auditoria para os seguintes eventos:

- a. Acesso feito por usuário a dados do portador do cartão;
- b. Ações tomadas por qualquer usuário com privilegio de administrador;
- c. Acesso aos registros de auditoria;
- d. Tentativas de acesso inválidas;
- e. Uso de mecanismos de identificação e autenticação;
- f. Inicialização dos logs de auditoria;
- g. Criação ou eliminação de objetos ao nível de sistema.

13. Os registros de auditoria deverão conter a identificação do Usuário, tipo de evento, data e hora, indicação de sucesso ou falha, origem do evento, identificação do dado, componente do sistema ou recurso afetado.

## **15. Atualização dos módulos.**

A atualização dos módulos do servidor SiTef bem como dos módulos *clientes* (Terminais) são disponibilizados através de acesso HTTPS com certificado válido Software Express, de forma a garantir o download de um lugar confiável. A segurança implementada no sistema para se evitar uma troca indevida se baseia em assinatura eletrônica, que quando violada tem a execução do módulo paralisada.

Quando o integrador realizar atualizações dos módulos do SiTef por meio de acesso remoto diretamente no servidor SiTef, a tecnologia utilizada para esta conexão deverá ser ativada somente quando necessária para o download, e desativada imediatamente após seu término.

## **16. Acesso remoto ao servidor SiTef para manutenção .**

Quando um suporte e/ou uma manutenção forem realizados de forma remota (em um servidor SiTef), deverão ser observados os seguintes itens:

- 1. Duplo fator de autenticação para acesso remoto. Utilizar Terminal Service TACACS+ (Terminal Access Controller Access-Control System Plus), com VPN (SSL/TLS ou IPSEC) com certificados individuais.

2. Habilitar criptografia ALTA para o protocolo RDP, utilizado pelo aplicativo *“Conexão de área de trabalho remota”*;
3. Não utilizar senhas padrões dos produtos e senhas exclusivas para cada cliente. Recomenda-se associar requisitos mínimos de complexidade de senha com requisitos de força (esforço/dificuldade para quebra da senha) em um só, e aumentar a flexibilidade nessas alternativas;
4. Permitir a conexão ao servidor SiTef somente de IP e *Mac address* conhecidos e específicos;
5. Alterar as senhas pelo menos a cada 90 dias;
6. As senhas deverão ter pelo menos 7 caracteres;
7. Utilizar senhas que contenham caracteres alfanuméricos;
8. Não permitir que a senha seja igual a uma das quatro últimas utilizadas;
9. Bloquear o ID do usuário no máximo após 6 tentativas incorretas;
10. Após o bloqueio pelo número de tentativas inválidas, zerar contagem somente após duração de, no mínimo, 30 minutos;
11. Bloquear o terminal ocioso por mais de 15 minutos;
12. Ter no servidor SiTef ativada a função de registro em log.
13. Os prestadores de serviços com acesso remoto às instalações do cliente, devem utilizar credenciais únicas de autenticação para cada cliente;
14. Manter informações sobre quais exigências do PCI-DSS são geridas por cada prestador de serviço, e quais são geridas pelas entidades (instituições);
15. Para prestadores de serviços, formalizar por escrito, acordo/confirmação que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do portador de cartão que possuam, ou caso contrário, não armazenar, não processar ou transmitir em nome dos clientes; ou ainda, conscientizá-los que eles podem ter impacto visto afetam a segurança do cliente mantendo um ambiente com dados do titular do cartão.



## 17. Anexo A - Desabilitando Serviços Desnecessários

Desabilitar serviços desnecessários, caso não estejam sendo utilizados por aplicações específicas:

Exemplo: Windows 2003

- ✓ Cliente DHCP
- ✓ Serviço de descoberta automática de Proxy da Web para WinHTTP
- ✓ Coordenador de transações distribuídas
- ✓ Gerenciamento de discos lógicos
- ✓ Serviços de transferência inteligente de plano de fundo
- ✓ Adaptador de desempenho WMI
- ✓ Agendador de Tarefas
- ✓ Detecção do hardware do Shell
- ✓ Acesso a dispositivos de interface humana.
- ✓ Ajuda e Suporte
- ✓ Alerta
- ✓ Alocador Remoto Procedure Call(RPC)
- ✓ Aplicativo de Sistema COM+
- ✓ Área de armazenamento.
- ✓ Armazenamento removível.
- ✓ Asp.Net State Service.
- ✓ Assistente de aquisição de imagens do Windows (WIA)
- ✓ Assistente de console de administração especial
- ✓ Áudio do Windows
- ✓ Cartão inteligente
- ✓ Centro de distribuição de chaves Kerberos
- ✓ Cliente da Web
- ✓ Serviço de Web
- ✓ Compartilhamento remoto da área de trabalho do NetMeeting
- ✓ Configuração sem Fio
- ✓ Conjunto resultante do provedor de diretivas
- ✓ Cópia de sombra de volume
- ✓ DDE de Rede
- ✓ Diretório de sessão dos serviços de terminal
- ✓ DSDM de DDE de rede
- ✓ Duplicação de arquivo
- ✓ Estrutura de driver do modo de usuário do Windows
- ✓ Extensões de driver de instrum. gerenc. do Windows.
- ✓ Firewall do windows/Compart. conexão c/ Internet (ICS)
- ✓ Fornecedor de suporte de segurança NT LM
- ✓ Gerenciador de conexão de acesso remoto automático
- ✓ Gerenciador de sessão de ajuda de área de trabalho remota
- ✓ Gerenciamento de aplicativo

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

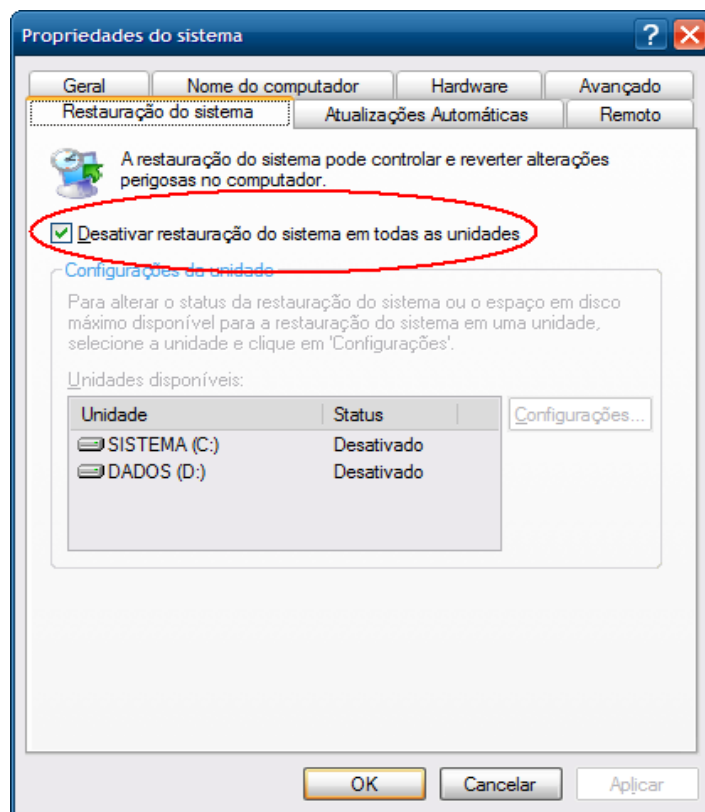
Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

- ✓ HTTP SSL
- ✓ Logon de rede
- ✓ Logs e alertas de desempenho
- ✓ Serviço de Mensageiro
- ✓ Mensagens entre Sites
- ✓ Microsoft Software Shadow Copy Provider
- ✓ Portable Media Serial Number Service
- ✓ Registro de licenças
- ✓ Registro Remoto
- ✓ Roteador e acesso remoto
- ✓ Serviço administrativo do gerenciador de disco lógico
- ✓ Serviço de configuração de rede.
- ✓ Serviço de disco virtual
- ✓ Serviço de indexação
- ✓ Serviço de FTP
- ✓ Serviço de Fax
- ✓ Serviço de Certificação
- ✓ Serviço de Instalação Remota
- ✓ Serviço de Redes (DNS, WINS,...etc)
- ✓ Serviço de UDDI
- ✓ Serviço de Windows Media Server
- ✓ Serviço de Impressão
- ✓ Spooler de impressão.
- ✓ Serviço VNC
- ✓ Serviço Gateway de camada de aplicativos
- ✓ Servidor de rastreamento de link distribuído
- ✓ Sistema de alimentação ininterrupta
- ✓ Sistema de arquivos distribuídos
- ✓ Telnet
- ✓ Temas
- ✓ Windows Installer

Quando do uso do **Windows XP, Win 7 e Win 8** deve-se também desativar a opção de restauração do sistema.

Acesse: Painel de controle → Sistema → clicar na guia '**Restauração do sistema**' e clicar em '**desativar restauração do sistema em todas as unidades**'



Em caso de exceções, descreva abaixo:

Exceções - Serviços Desabilitados	
Nome do Serviço	
Justificativas	
Aprovado por	

Exceções - Serviços Desabilitados	
Nome do Serviço	
Justificativas	
Aprovado por	

Exceções - Serviços Desabilitados	
Nome do Serviço	
Justificativas	
Aprovado por	

## 18. Anexo B - Atualizações e Patches de Segurança

### ATUALIZAÇÕES E PATCHES DE SEGURANÇA

1.0 – Data da Atualização	
Data da atualização	<DDMMAAA>

2.0 – Responsável pela Atualização	
Nome Completo	<Nome Completo>
Departamento	<depto>
Ramal/Contato	<ramal ou telefone de contato>

3.0 – Motivo da Atualização		
3.1	Motivo:	<input type="checkbox"/> Atualização Periódica <input type="checkbox"/> Atualização Emergencial <input type="checkbox"/> Recomendações do Fabricante <input type="checkbox"/> Correções de Problemas ou Falhas <input type="checkbox"/> Outros (especificar):
3.2	Autorizado por	<input type="checkbox"/> Diretor <input type="checkbox"/> Gerente <input type="checkbox"/> Supervisor <input type="checkbox"/> Nome do Responsável: < nome>  <u>Assinatura do responsável:</u>

4.0 – Detalhamento da Atualização	
Descrição:	

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*


### 5.0 – OBSERVAÇÕES – Atualização *(Opcional)*


### 6.0 – Estado Final

**Realizado com Sucesso?**

- ☐ Sim  
☐ Não

### 7.0 – OBSERVAÇÕES – Estado Final *(Obrigatório em caso negativo)*


### 8.0 – Atitude Tomada *(Obrigatório em caso negativo)*


## 19. Anexo C – Solicitação de alteração de ambiente

### SOLICITAÇÕES / ALTERAÇÕES

<b>1.0 – Data da Solicitação de alteração</b>		
<b>Data da Solicitação</b>	<DDMMAAA>	
<b>3.0 – Dados do Cliente</b>		
<b>Nome da Empresa</b>	<Nome da Empresa>	
<b>3.0 – Dados do Solicitante</b>		
<b>Nome do Solicitante:</b>	<Nome completo>	
<b>Tipo</b>	.... <input type="checkbox"/> Interno .... <input type="checkbox"/> Externo	
<b>Telef./Ramal do solicitante:</b>	<Tel/ramal>	
<b>4.0 – Dados da Mudança (Preenchido pelo solicitante)</b>		
4.1	Classificação:	<input type="checkbox"/> Programada <input type="checkbox"/> Não-Programada <input type="checkbox"/> Emergencial
4.2	Motivo:	<input type="checkbox"/> Atualização de versão <input type="checkbox"/> Solicitação do cliente <input type="checkbox"/> Novas implementações e melhorias <input type="checkbox"/> Outros (especificar):
4.3	Tipo:	<input type="checkbox"/> Hardware <input type="checkbox"/> Sistema Operacional <input type="checkbox"/> Aplicação <input type="checkbox"/> Rede <input type="checkbox"/> Segurança <input type="checkbox"/> Infra-estrutura <input type="checkbox"/> Outros (especificar):
2.4	Descrição da alteração:	<descrição do que será alterado nesta solicitação>

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobreloja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

www.softwareexpress.com.br

--	--	--

5.0 – Indisponibilidade de Ambiente <i>(Preenchido pelo solicitante)</i>		
5.1	Hora Início (hh:mm):	
5.2	Tempo Total de Execução (hh:mm)	
5.3	Tempo Total de Paralisação (hh:mm)	
5.4	Tempo Total de Plano de Volta	

6.0 – Severidade <i>(Preenchido pelo solicitante)</i>	
6.1	<input type="checkbox"/> Crítica <input type="checkbox"/> Grande Impacto <input type="checkbox"/> Impacto Alto <input type="checkbox"/> Pequeno Impacto <input type="checkbox"/> Sem Impacto  Motivo: <Descrição>

7.0 – Descrição Passo a Passo das Alterações <i>(Preenchido pelo solicitante)</i>	
7.1	
7.2	
7.3	
7.4	
7.5	
7.6	

8.0 – Dados do Técnico que efetuou o Procedimento <i>(Preenchido pela Operação)</i>	
Nome do técnico:	<Nome completo>
Telef./Ramal do técnico:	<Tel/ramal>

9.0 – Aprovação do Procedimento de Alteração <i>(Preenchido pelo Avaliador)</i>		
10.1	Avaliador	<input type="checkbox"/> • Diretor <input type="checkbox"/> • Gerente <input type="checkbox"/> • Supervisor de Operação
10.2	Aprovação da mudança	<input type="checkbox"/> • Autorizado <input type="checkbox"/> • Não autorizado  Motivo: <Descrição>



		Assinatura do Responsável:

**11.0 – Data da atualização**

<b>Data da Solicitação</b>	<DDMMAAA>
----------------------------	-----------

**12.0 – OBSERVAÇÕES**

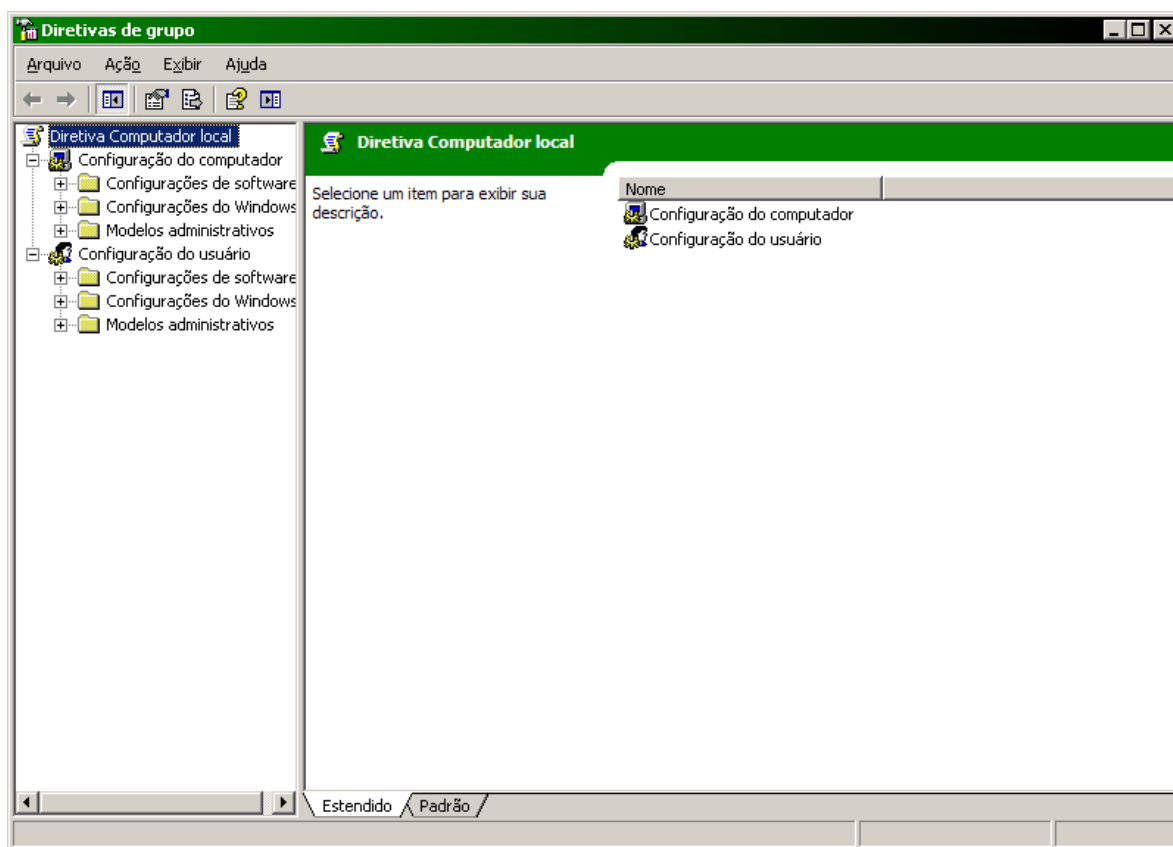
--

## 20. Anexo D - Configuração do Sistema operacional Windows para logon/auditoria.

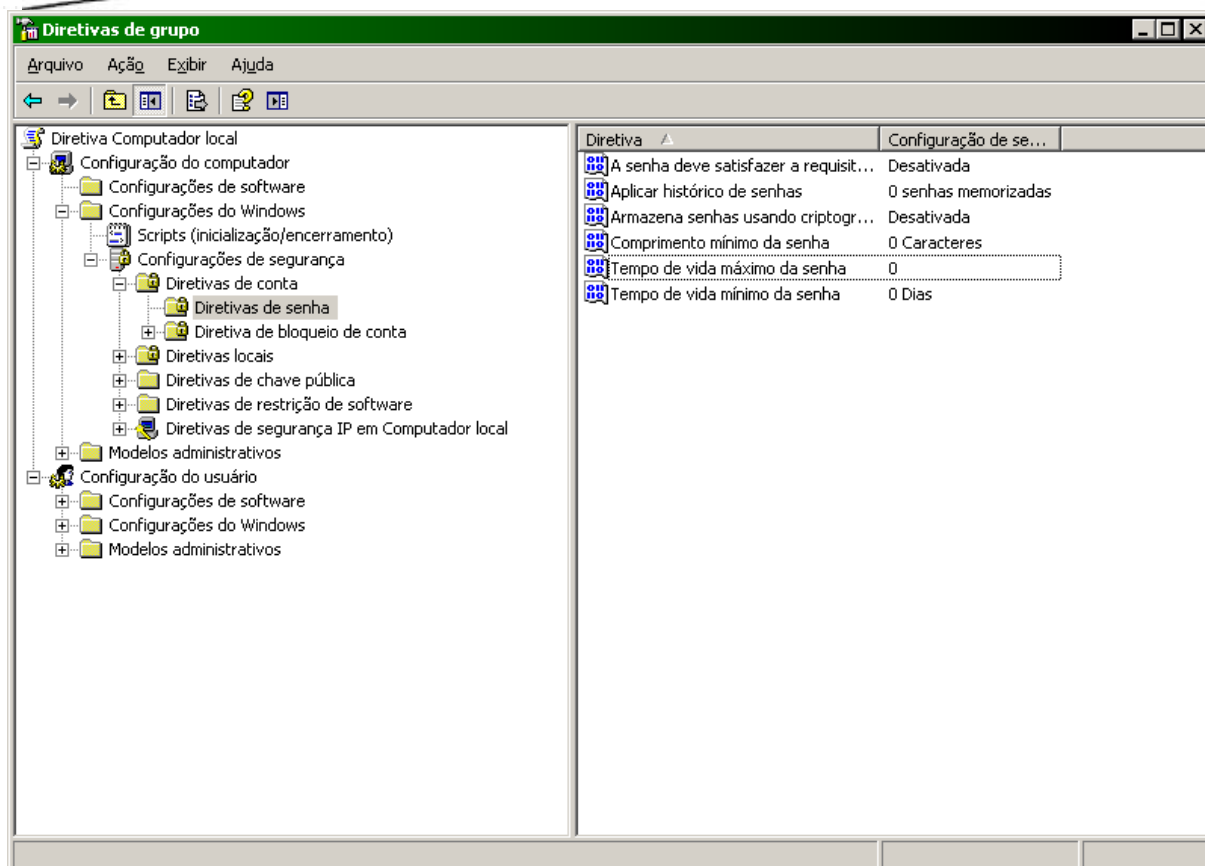
Exemplo de configuração das Políticas de segurança no Windows 2000 e 2003.

Acesse: Iniciar → Executar → digite **gpedit.msc** e tecla <enter>.

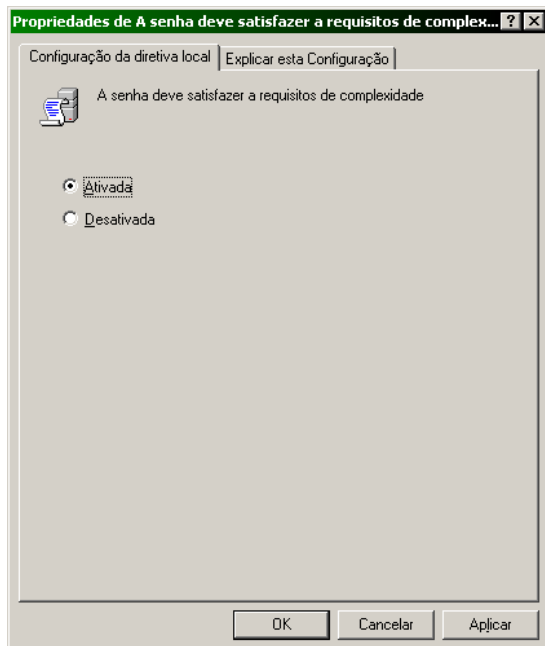
Aparecera a tela abaixo:



Nas opções a esquerda escolha configurações do computador → Configurações do Windows → Diretivas de conta → Diretivas de senha. A tela abaixo será exibida:



Clique na opção à esquerda “A senha deve satisfazer os requisitos de complexidade” e selecione a opção “Ativada” conforme tela abaixo:



Realize este procedimento em todas as opções abaixo;

Aplicar histórico de senhas

Selecionar a opção: 4

Comprimento mínimo da senha

Selecione a opção: 7

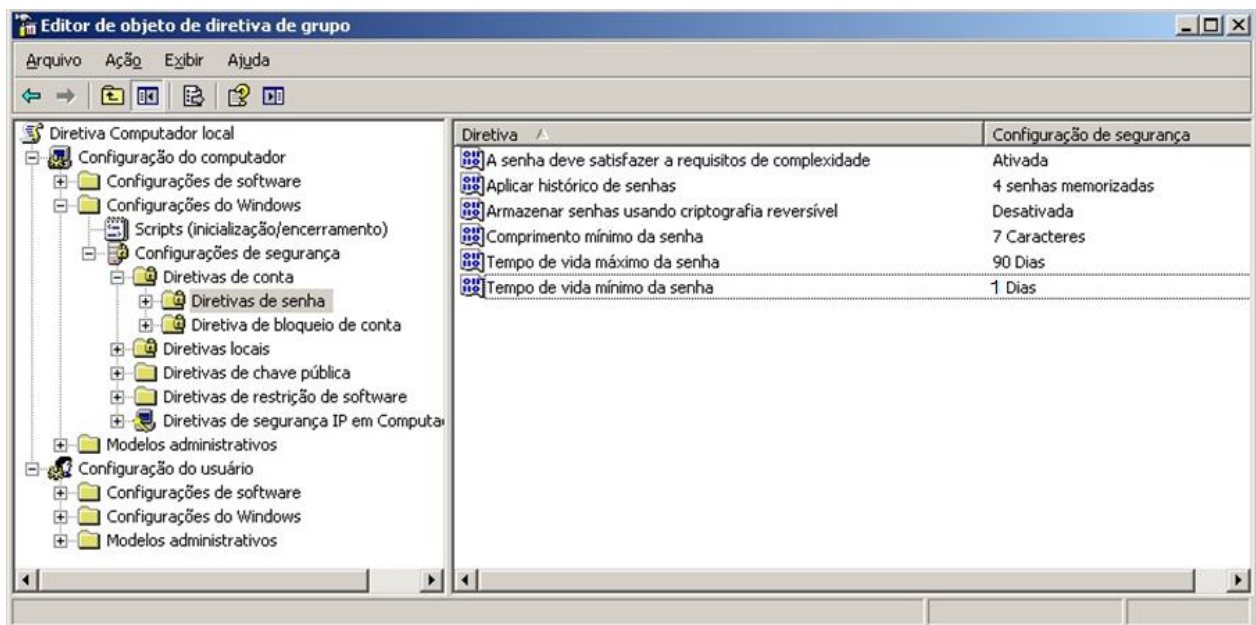
Tempo de vida máximo da senha

Selecione a opção: 90

Tempo de vida mínimo de senha

Selecione a opção: 1

Após todas as configurações, as diretivas devem ficar conforme a tela abaixo:



Clique na opção a esquerda “Diretiva de bloqueio de conta”

Clique na opção a esquerda “limite de bloqueio de conta”;

Selecionar a opção: 6.

clicar em OK

Selecionar a opção “Duração do bloqueio de conta”

Selecionar:1

Conforme tela abaixo:

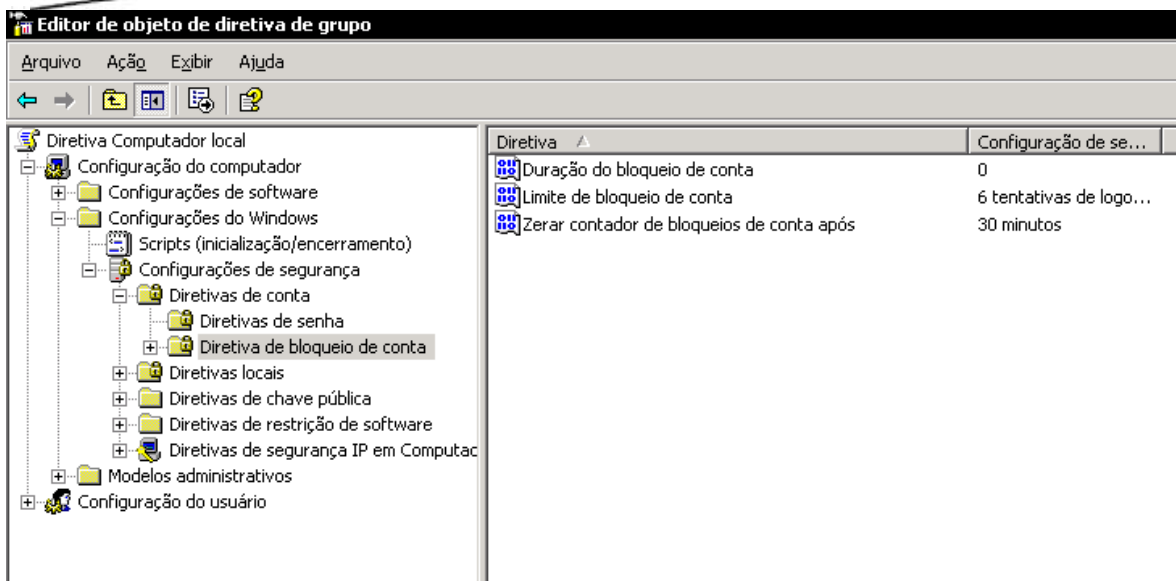
*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

www.softwareexpress.com.br

Versão 1.5

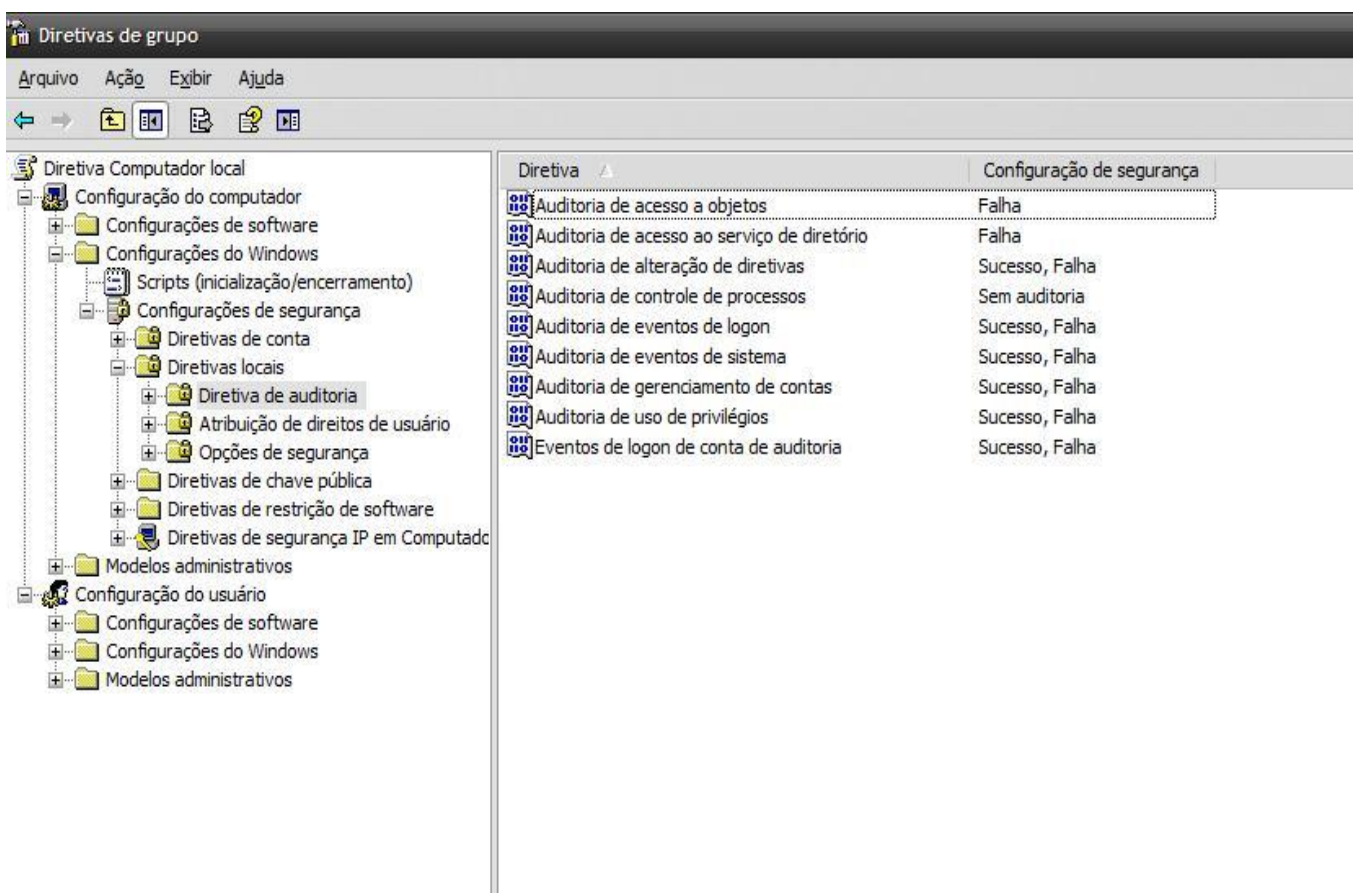
Pag. 33



Em seguida nas opções a esquerda clicar em: Diretivas locais → Diretiva de auditoria

Clicar na opção à esquerda “Auditoria de logon”.

Selecionar “êxito (sucesso)” e “falha”, conforme tela abaixo:



*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

Versão 1.5

Pag. 34

Após passo anterior selecione a opção do lado esquerdo em: Configurações do usuário → modelos administrativos → Painel de controle → Exibição

Clique em “Proteção de tela”  
Selecione: Ativado

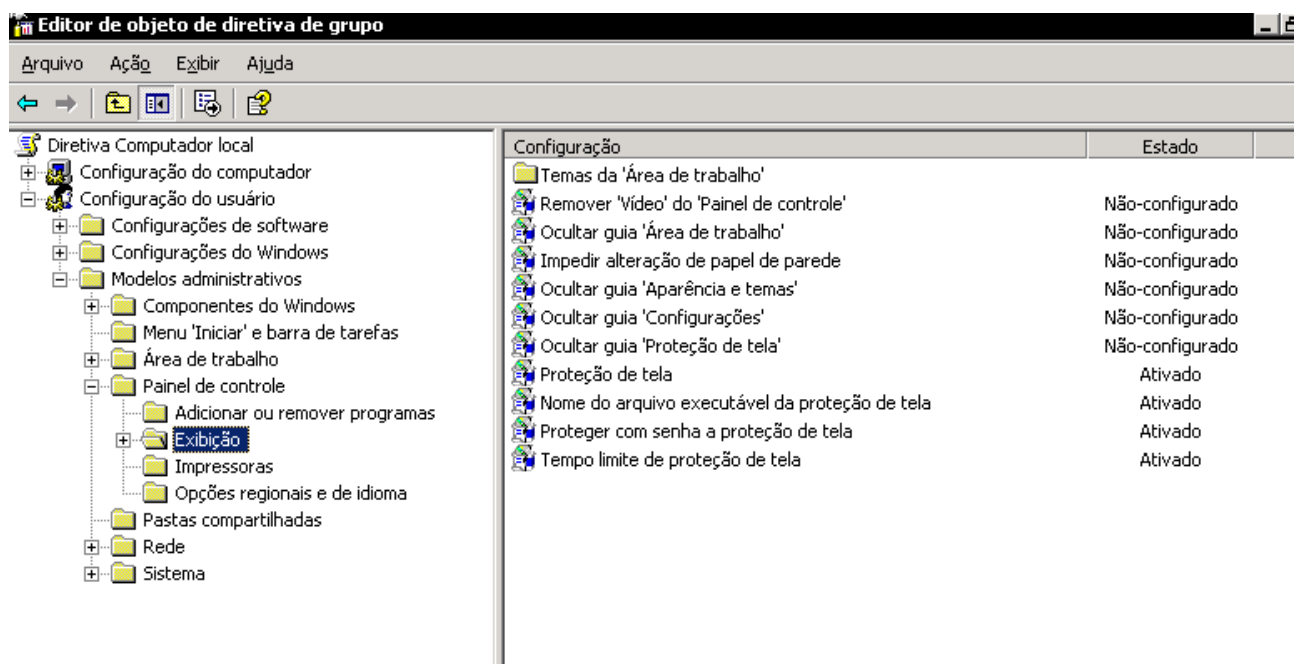
Clique em “Nome do arquivo executável da proteção de tela”  
Selecione: Ativado

Em “nome do arquivo executável”, coloque o caminho de um protetor de tela  
Exemplo: c:\Windows\system32\logon. scr

Clique em “Proteger com senha a proteção de tela”  
Selecione: Ativado

Clique em “tempo de proteção de tela”  
Selecione: Ativado  
Tempo de espera em segundos selecione 900.

Conforme a tela abaixo:



*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

## 21. Anexo E - Sincronização de horário no servidor Windows 2000, XP e 2003

### Exemplo de sincronização de tempo no Windows.

Configurando no Windows 2000 e 2003 Server (O servidor de Horas)

É necessário possuir um servidor NTP disponível na rede ou localizar um na Internet (Informações em <http://www.ntp.org/>)

1. Abra um prompt de comando.

Digite: "**sc config w32time start= auto**" ou habilite o serviço "Horário do Windows"

2. Digite: "**net time /setsntp:<endereço>**" onde <endereço> por ser o endereço ip do servidor NTP da rede ou servidor NTP disponível na internet.

Exemplo: net time /setsntp:192.168.0.1 ou net time /setsntp:time.windows.com

3. Agora digite: "**net stop w32time**" e "**net start w32time**"

Para visualizar quem é seu servidor de horas, digite "**net time /querysnTP**".

**Obs.:** As estações Windows, por default se estiverem em domínio atualizam a hora automaticamente no servidor Windows Server.



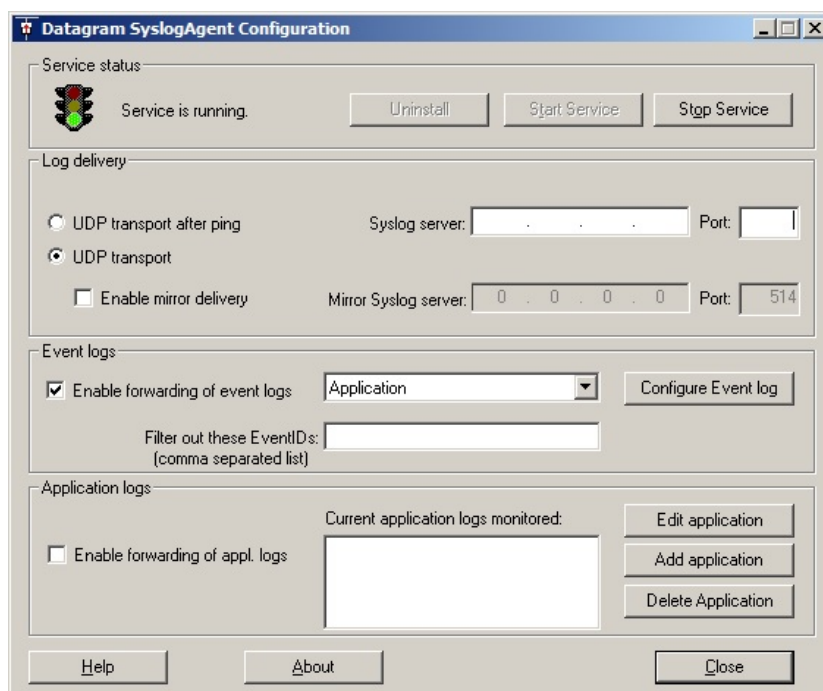
## 22. Anexo F – Configurando Exportação de Log do Sistema

### Exemplo - Configurando aplicativo SysLog

Note que, este aplicativo (SysLog) não foi desenvolvido pela Software Express e portanto, a mesma **não dará suporte a esta aplicação**.

Seguem abaixo as principais telas de configuração deste aplicativo, bem como, parâmetros de configuração necessários para que a exportação seja configurada com sucesso.

- 1- Defina um IP remoto (Servidor que irá receber esses log's) e utiliza a **porta 514** (porta padrão oficial do aplicativo SysLog)



- 2- Parâmetros configurados em “Configure Event Log”



*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

Versão 1.5

Pag. 37

## 23. Mantendo políticas perante Clientes e Integradores

### 22.1. Como o Guia de Implementação é distribuído?

O guia de implementação é distribuído via e-mail (arquivo **PDF**) em cursos internos, instalações e solicitações dos clientes, e após alterações e/ou liberação de novas versões.

### 22.2. Quem distribui o *Guia de Implementação*?

A *Software Express Informática* disponibiliza este guia juntamente com o software SiTef.

### 22.3. Onde este assunto é tratado neste documento?

Este assunto é abordado no **item 13 – Políticas de Segurança** deste documento.

### 22.4. Qual a periodicidade com a qual o *Guia de Implementação* é atualizado?

É atualizado anualmente, agregando as ultimas alterações e recomendação do PCI-DSS/PA-DSS.

## 24. Histórico de alterações

Data	Versão	Descrição
20/10/2009	1.3	Criação do documento
04/02/2010	1.4	Atualização de acordo com as normas PCI-DSS 2.0
17/02/2014	1.5	Atualização de acordo com as normas PCI-DSS 3.0

## 25. Glossário

### A

#### **ABNT**

A Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normatização técnica no Brasil, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro. Trata-se de uma entidade privada e sem fins lucrativos fundada em 1940.

#### **Adware**

Do Inglês **Advertising Software**. Software especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

#### **Antivírus**

Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

#### **Assinatura digital**

Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

#### **Atacante**

Pessoa responsável pela realização de um ataque. Veja também Ataque.

#### **Ataque**

Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

#### **Autoridade certificadora**

Entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

### C

#### **Certificado digital**

Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Veja também Assinatura digital.

#### **Conexão segura**

Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

#### **Criptografia**

Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

#### **Cifrar**

Se valer de caracteres, palavras ou sinais para codificar informações confidenciais.

## D

### Data Center

Empresas especializadas em prover todo ambiente de TI necessário para empresas que utilizem informática e/ou a Internet. Os Data Centers são construídos para atender aos mais exigentes níveis de serviço, tanto na qualidade de equipamentos como nas equipes e processos de operação e manutenção.

## F

### Firewall

Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

## G

### GLBA

A Lei Gramm-Leach-Bliley, promulgada em 1999, define o que as empresas de serviços financeiros podem fazer com as informações pessoais confidenciais que coletam durante suas atividades de consultoria de investimentos.

## H

### Hacker

Pessoa responsável pela realização de um ataque. Veja também Ataque. Verificar Atacante

### HIPAA

A Lei norte-americana Health Insurance Portability and Accountability Act (HIPAA), aprovada em 1996 e dedicada à proteção de dados do portador do cartão, refere-se especialmente há os aspectos da integridade e da disponibilidade

### HTTP

Do Inglês *HyperText Transfer Protocol*. Protocolo usado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o *browser*).

### HTTPS

Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

## I

### ID

Nome do usuário, é o endereço que representa uma identidade ou uma conta pessoal em um computador.

### IDS

Do Inglês *Intrusion Detection System*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

### IEEE

Acrônimo para *Institute of Electrical and Electronics Engineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletro-eletrônicos.

### Invasão

Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

## IPSec

Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPSec) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja a mesma da origem)

## L

### Log

Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidente de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

## N

### NTP

É um protocolo para sincronização dos relógios dos computadores baseado no UDP (TCP/IP), ou seja, ele define um jeito para um grupo de computadores conversar entre si e acertar seus relógios, baseados em alguma fonte confiável de tempo. Com o NTP é fácil manter o relógio do computador sempre com a hora certa, com exatidão por vezes melhor que alguns milésimos de segundo.

## P

### Proxy

Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

## R

### RDP

Remote Desktop Protocol (ou somente RDP) é um protocolo multi-canal que permite que um usuário conecte a um computador rodando o Microsoft Terminal Services. Existem clientes para a maioria das versões do Windows, e outros sistemas operacionais como o Linux. O servidor escuta por padrão a porta TCP 3389.

### Rede sem fio

Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

### ROLLBACK

Desfaz os procedimentos executados anteriormente, fazendo com que todas as modificações realizadas sejam retornadas a origem.

## S

### Scan

Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*.

### Scanner

Programas utilizados para efetuar varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

### SSH

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Do Inglês **Secure Shell**. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

## SSID

Do Inglês **Service Set Identifier**. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

## SSL

Do Inglês **Secure Sockets Layer**. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Veja também HTTPS.

## SOX

Lei Sarbanes-Oxley, conhecida também como SOX, é uma lei americana promulgada em 30/06/2002 pelos Senadores Paul Sarbanes e Michael Oxley. Nela estão envolvidas as empresas que possuem capitais abertos e ações na Bolsa de NY e Nasdaq, inclusive várias empresas brasileiras estão se adequando a esta Lei, basicamente trata da integridade, garantindo que os relatórios financeiros sejam completos e precisos ou pelo menos garantindo a precisão dos controles que os geram.

## Stand Alone

Um computador com uma cópia idêntica de outro sendo atualizado em tempo real.

## SNMP

(do inglês Simple Network Management Protocol - Protocolo Simples de Gerência de Rede) é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores

### SNMP Community String (String de comunidade)

Uma *string* é enviada juntamente com a solicitação SNMP. Se correta o dispositivo (por exemplo, um router) responde com as informações solicitadas. Se incorreta o dispositivo descarta o pedido e, simplesmente, não responde);

SNMP Community Strings são utilizados apenas por dispositivos que suportam protocolo SNMPv1 e SNMPv2c. Para SNMPv3 usa-se autenticação do nome de usuário/senha, juntamente com uma chave de criptografia.

## SYSLOG

É um padrão criado pela IETF para a transmissão de mensagens de log em redes IP. O termo é geralmente usado para identificar tanto o protocolo de rede quanto para a aplicação ou biblioteca de envio de mensagens no protocolo syslog. O protocolo syslog é muito simplista: o remetente envia uma pequena mensagem de texto (com menos de 1024 bytes) para o destinatário (também chamado "syslogd", "serviço syslog" ou "servidor syslog"). Tais mensagens podem ser enviadas tanto por UDP quanto por TCP. O conteúdo da mensagem pode ser puro ou codificado por SSL. O protocolo syslog é tipicamente usado no gerenciamento de computadores e na auditoria de segurança de sistemas. Por ser suportado por uma grande variedade de dispositivos em diversas plataformas, o protocolo pode ser usado para integrar diferentes sistemas em um só repositório de dados.

# V

## Vírus

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

## VPN

Do Inglês **Virtual Private Network**. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

*Este documento possui informações e tecnologia de propriedade exclusiva da Software Express. As informações aqui contidas não podem, a não ser quando autorizado previamente e por escrito pela Software Express Informática Ltda, ser reproduzido, utilizado ou divulgado por qualquer meio ou modo, total ou parcialmente, para qualquer outro fim que não seja o de servir de meio de consulta para a criação de módulos que façam interface com soluções desenvolvidas pela Software Express.*

Av. Paulista, 2202 Sobrelaja H Cep 01310-300 PABX - (11) 3170 5300 FAX- (11) 31705301

[www.softwareexpress.com.br](http://www.softwareexpress.com.br)

## Vulnerabilidade

Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um rede de computadores .

## W

### WEP

Do Inglês **Wired Equivalent Privacy**. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

### Wi-Fi

Do Inglês **Wireless Fidelity**. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

### WLAN

Do Inglês **Wireless Local-Area Network**. Refere-se a um tipo de rede que utiliza ondas de rádio de alta frequência, ao invés de cabos, para a comunicação entre os computadores.

### WPA

Do Inglês **Wi-Fi Protected Access**. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Esta tecnologia foi projetada para, através de atualizações de *software*, operar com produtos Wi-Fi que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.