

GUIA DE IMPLEMENTAÇÃO

SiTef 7.0.XX.XXX - PA-DSS 3.2

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 como guia de implementação PA-DSS do SiTef.

Índice

1. PCI	3
2. SiTef	4
2.1. SiTef e Clients - Versões e Sistemas Operacionais	5
2.2. Conexões SiTef	6
3. Rede Segura	6
4. Armazenamento de Dados do Cliente	7
5. Transmissão de dados do portador do cartão	7
6. Log de Eventos	8
6.1. Opções de Auditoria/Registro no Windows	8
6.2. Auditoria de Segurança com políticas de Auditoria Central	9
6.3. Opção de registros centralizados	10
7. Contas de usuários	11
7.1. Configuração de Contas do Windows	12
8. Chaves internas de criptografia	16
9. Metodologia de Versionamento SiTef	17
10. Atualização dos Módulos	18
11. Instruções gerais e informações	19
11.1. Definições de armazenamento de dados do portador do cartão	19
11.2. Backups	21
11.3. Considerações relevantes para um Rede Segura	21
11.4. Considerações sobre Redes Wireless	23
11.5. Gerenciamento de Vulnerabilidades	25
11.6. Monitoração e armazenamento de logs	26
11.7. Plano de respostas a incidentes	27
11.8. Política de Segurança	28
11.9. Contas de Usuário	28
11.10. Habilitando Serviços Necessários	29
11.11. Sincronização de horário no servidor Windows Server 2016	30
11.12. Mantenha as políticas com Clientes e Integradores	30
12. Referencias do PA-DSS 3.2 no Guia de Implementação	31
13. Histórico de Alterações	32
14. Glossário	33

1. PCI

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.

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 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 componentes do sistema são definidos como qualquer componente do servidor ou aplicação da rede, incluído ou conectado ao ambiente que manipulam ou transitam os dados do portador do cartão. A segmentação adequada da rede, é aquela que separa os sistemas que armazenam, processam ou transmitem os dados do portador do cartão daqueles que não o fazem. Procure reduzir a extensão do ambiente dos dados do portador do cartão. (Use firewalls, switches, routers, etc.).

O padrão do PCI-DSS é dividido em seis categorias, tendo sempre como intuito proteger os números dos 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;

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 como guia de implementação PA-DSS do SiTef.

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/>.

2. SiTef

O **SiTef** é uma aplicação TEF (Transferência Eletrônica de Fundos) e atua como meio de pagamento (aplicação middleware) responsável pela comunicação das operações de pagamento (transações eletrônicas) entre o varejo e as redes adquirentes de cartão.

Uma transação **TEF** exige uma série de informações, como valor e outros tipos de dados solicitados em especificação técnica definida por cada rede adquirente. O **SiTef** foi desenvolvido para coletar o mínimo de informações necessárias para se efetuar uma transação. Tudo ocorre de modo a simplificar seu próprio funcionamento e a respeitar as especificações enviadas por cada uma das diversas redes adquirentes.

O **Terminal**, também identificado como PDV (Ponto de Vendas ou Ponto de check-out) de um estabelecimento comercial, detém uma aplicação de software que permite a captura de dados do titular do cartão para realização de uma transação financeira ou de uma consulta a cheques, criando assim transações de consultas, débitos e créditos, na troca de bens entre um comerciante e um cliente. Além do PDV coletar os dados das transações, este deverá exibir a resposta e imprimir o cupom TEF.

A solução **TEF** da Software Express é composta pelo servidor SiTef e dois tipos de interfaces Clients, identificadas como *CliSiTef* e *Cliente SiTef Modular*, as quais são escolhidas pela empresa desenvolvedora da aplicação de frente de caixa (PDV) conforme conveniência de desenvolvimento (a desenvolvedora é também chamada de Automação Comercial).

Quanto à criptografia **AES**, ela utiliza uma chave de 128 bits montada dinamicamente durante a execução do módulo no **SiTef** (esta chave não está gravada no código fonte) é um

vetor de inicialização gerado dinamicamente a cada transação, e se utiliza de uma informação que os dois lados conhecem (Transmissor e Receptor, das versões Clients e do SiTef Server).

O servidor **SiTef** deve ser instalado em um servidor dedicado. Neste servidor o acesso para a internet deve estar bloqueado, e pode ser liberado apenas em momentos de atualizações do sistema operacional ou antivírus.

O mesmo se aplica aos PDVs (CliSiTef e Cliente SiTef Modular), o equipamento deve ser isolado da internet, mas com antivírus e sistema operacional regularmente atualizados. No caso de PDVs em terminais Android POS, a determinação dos aplicativos que são instalados e o sistema de assinatura dos aplicativos, bem como o hardening de segurança e atualização do sistema operacional/componentes de segurança, são definidos pelo fabricante do terminal.

O antivírus deve ser instalado no servidor SiTef, porém para melhor performance, sugerimos a criação de filtros eliminando a varredura dos diretórios e subdiretórios da árvore SiTef, exceto pelo diretório "SiTef\Aplic.win", que deverá ser verificado.

O SiTef não possui requisitos de banco de dados ou componentes adicionais de Sistema Operacional.

Algumas recomendações para checar:
Requisitos mínimos de hardware

- Microcomputador com S.O Windows compatível;
- 4 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);

2.1. SiTef e Clients - Versões e Sistemas Operacionais

Server Windows (SiTef)

- Windows 2016 Server – 64 bits

Client Windows (CliSiTef.dll e Cliente SiTef Modular)

- Windows 10 – 32 e 64 bits

Client Linux (CliSiTef.so)

- CentOS 7.6 – 32 e 64 bits
- Ubuntu 18.04 – 32 e 64 bits

Client POS Android (libclisitef.so)

- Gertec GPOS700 (WPOS-3)
- Ingenico A8
- Verifone Carbon

Indicamos **Serviços** necessários:

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 como guia de implementação PA-DSS do SiTef.

- 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).

2.2. Conexões SiTef

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

Porta utilizada na comunicação entre **SiTef-Adquirentes**: Não existe um padrão definido, estas portas devem ser definidas entre as partes (área de infraestrutura e 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**.

3. Rede Segura

O cliente deve implementar uma rede segura a fim de proteger sua rede de pagamento de qualquer acesso não autorizado oriundos de outras redes, seja interna ou externa.

A comunicação entre o servidor SiTef e as redes adquirentes segue as normas de comunicação disponíveis e exigidas por cada rede adquirente, seja via link X.25 ou TCP/IP, utilizando-se de algoritmos de criptografia, VPN, Certificados, ou qualquer outra forma segura de comunicação aceito pelo PCI-DSS.

Para comunicação entre o servidor SiTef e redes adquirentes, é recomendada a utilização de link dedicado usando protocolo X25 ou usando uma rede considerada privada, pois no mercado Brasileiro, o link X.25 (link dedicado contratado) não possui saída para Internet. Caso a comunicação seja via protocolo TCP/IP, o cliente deve considerar proteger esta comunicação, por exemplo, implementando criptografia TLS 1.2 e VPN/IPSEC usando algoritmos de criptografia forte e uso apenas de chaves confiáveis ou certificado aceito pelo PCI-DSS (regulamentação atual).

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);

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 como guia de implementação PA-DSS do SiTef.

- ✓ Link TCP via internet (redes públicas): Obrigatoriamente, criar uma VPN/IPSec e, utilizar algoritmos de criptografias e chaves aceitas pelo PCI-DSS (normas vigentes);

4. Armazenamento de Dados do Cliente

O **PAN** (*Primary Account Number*) do cartão, o número impresso no cartão, poderá ser armazenado pelo SiTef apenas para algumas adquirentes, pelo período da transação sempre criptografado utilizando-se o padrão (AES 128 bits).

Os relatórios de transações é a única interface disponível para monitorar as transações do portador do cartão, apresentando o PAN do cartão truncado (visíveis somente os 6 primeiros e os 4 últimos dígitos). O SiTef não oferece opção para que este tipo de visualização seja alterado.

O período de retenção dos arquivos no SiTef é definido por padrão em 45 dias para arquivos de LOG e 20 dias para arquivos AUDIT. O SiTef automaticamente expurga de modo seguro esses arquivos depois que este período é alcançado. Se o cliente usa outro sistema para armazenar dados de cartão, ele deve implementar procedimentos para garantir o expurgo de modo seguro após excedido o período de retenção desses dados.

Arquivos de LOG estão localizados em: \\SiTef\Log\LOG_MMDD.DAT;

Arquivos de AUDIT estão localizados em \\SiTef\Audit\MMDDhhmm.XXX, onde:

MM=mês;

DD=Dia;

hh=hora;

mm=minuto;

XXX = extensão adotada para cada Adquirente (**051**=Vero, **125**=Cielo, **181**=GetNetLac, etc).

Note que, o arquivo de LOG pode conter o PAN criptografado temporariamente no diretório \\SiTef\LOG.

5. Transmissão de dados do portador do cartão

O SiTef não disponibiliza o envio dos dados do portador do cartão por tecnologias de mensagem ao usuário final (por exemplo, e-mails) e o suporte da Software Express Informática não coleta junto aos seus clientes, dados de autenticação confidenciais (*SAD-Sensitive Authentication Data*) em seu processo de atendimento via suporte técnico.

É importante salientar que **nunca** se deve enviar o PAN de forma não codificada. Caso necessário este envio através de e-mail, o procedimento é gravar metade desta informação em um arquivo texto, compactá-lo com senha (utilizando algoritmos fortes de encriptação) e enviá-lo ao destinatário. A outra parte do PAN deve ser enviada em um segundo e-mail, ambos utilizando um algoritmo de *criptografia forte* ou outras tecnologias de mensagem de usuário final (as senhas devem ser enviadas por outro meio, por exemplo, por telefone). O receptor da mensagem deve recompor a mensageria e obter o PAN apenas em ambiente seguro.

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 como guia de implementação PA-DSS do SiTef.

Módulos do SiTef que se comunicam com as adquirentes usando método webservice, devem ter a utilização de um *certificado digital*, o qual deve ser comprado de uma C.A de mercado (Autoridade Certificadora). Isto irá tornar a comunicação entre SiTef e adquirentes segura. Feito um download deste certificado em um diretório disponível no servidor SiTef, este caminho deve ser indicado nas configurações da aplicação.

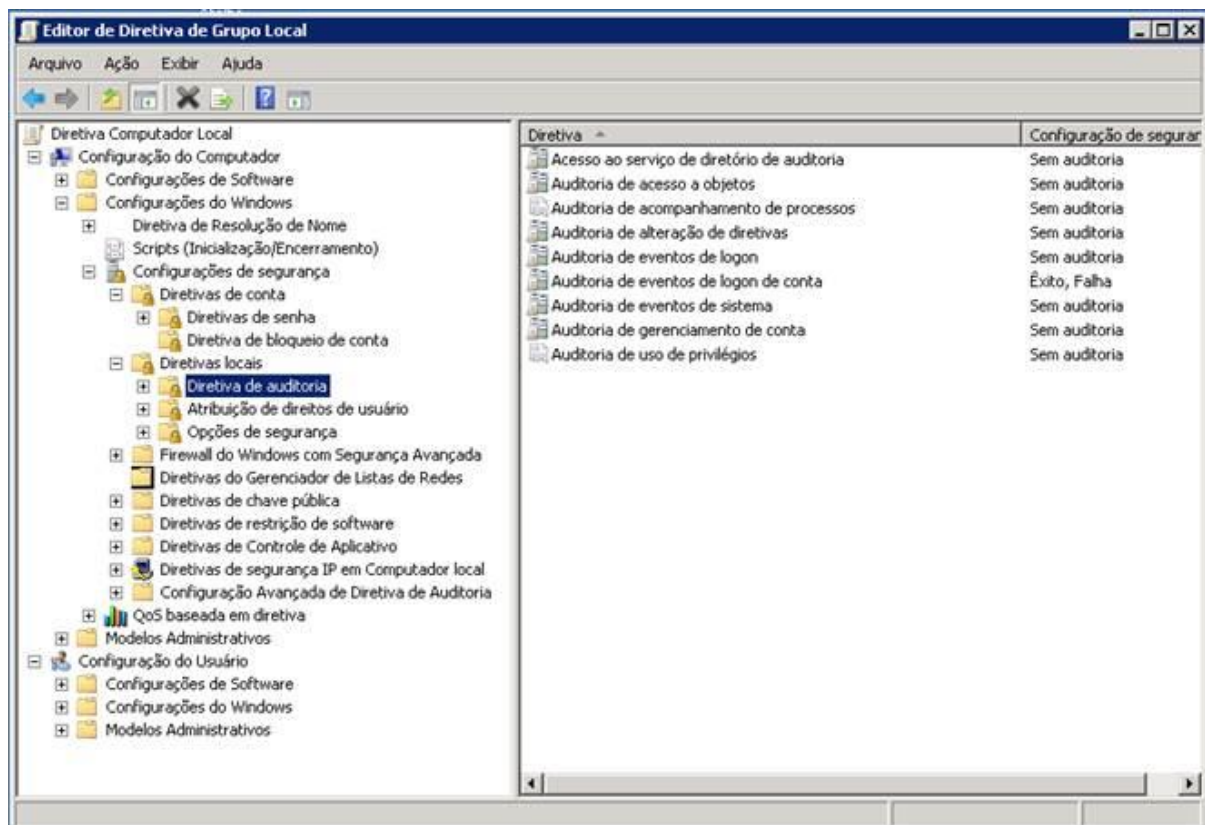
6. Log de Eventos

O registro de informações de auditoria está sempre ativo por padrão e integrado ao Microsoft Event Viewer.

6.1. Opções de Auditoria/Registro no Windows

Habilitando log de auditoria no Windows Server para o SiTef:

1. Clique no menu “Iniciar”, “Executar”, digite “**gpedit.msc**” e pressione “<enter>”;
2. Do **lado esquerdo** da tela, escolha “Configuração do Computador”, “Configurações do Windows”, “Configurações de Segurança”, “Diretivas Locais”, “**Diretiva de Auditoria**”;
3. Clique do **lado direito** na opção “Auditoria de Eventos de Logon”. Selecione “Com ou Sem Auditoria”.



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 como guia de implementação PA-DSS do SiTef.

6.2. Auditoria de Segurança com políticas de Auditoria Central

Ativando políticas de auditoria centrais no diretório SiTef, criando uma política de acesso a objetos global.

1. Entre no controlador de domínio ou servidor **SiTef** como uma conta **<dominio>\Administrador** com uma senha forte. **Administrador Local**: uma **senha forte**;
2. No Gerenciador do Servidor, aponte para **Ferramentas** e clique em **Gerenciamento de Política de Grupo**. Ou **Administrador Local**: Windows → Executar → gpedit.msc;
3. Na árvore do console, clique duas vezes em **Domínios**, clique duas vezes em **<dominio>**, clique em **<domínio>** e clique duas vezes em **Servidores de Arquivos**. Ou **Administrador Local**: Configurações do Windows → Configurações de Segurança → Políticas Locais;
4. Clique com o botão direito do mouse na política escolhida e clique em **Editar**;
5. Clique duas vezes em **Configuração do Computador**, clique duas vezes em **Políticas** e clique duas vezes em **Configurações do Windows**;
6. Clique duas vezes em **Configurações de Segurança**, acesse **Políticas Locais** e clique duas vezes em **Política de Auditoria** (clique duas vezes em **Políticas de Auditoria**);
7. Clique duas vezes em **Auditoria de Acesso a Objeto**;
8. Habilite **Configurar estes eventos**, marque as caixas de seleção **Êxito** e **Falha** e clique em **OK**;
9. Marque a caixa de seleção **Definir esta configuração de política** e clique em **Configurar**.

Atualizar as configurações de Política de Grupo

10. Entre no servidor SiTef com uma conta **<dominio>\Administrador** com uma senha forte. Para **Administrador Local** após a configuração as diretivas já estarão habilitadas.
11. Pressione a tecla do **Windows+R** e digite **cmd** para abrir uma janela do **Prompt de Comando**.
12. Digite **gpupdate /force** e pressione **ENTER**.

6.3. Opção de registros centralizados

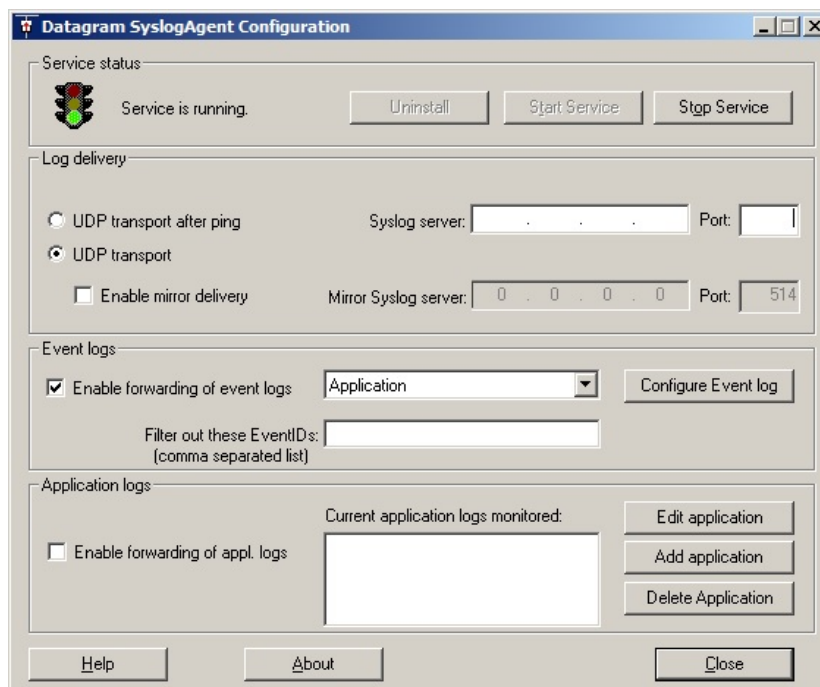
O SiTef tem como padrão a gravação dos eventos nos arquivos de log do Windows, possibilitando o acesso a estes dados através do visualizador de eventos do próprio Windows. É recomendável que este log de eventos seja armazenado em um outro servidor, para esta exportação é recomendado o uso do agente Syslog.

Como os logs do SiTef fazem parte do serviço de log do Windows, não há restrições quanto ao uso de mecanismos de log centralizados capazes de ler logs em formato Windows ou de processar eventos em formato syslog, como os SIEMs usados pelo mercado, seja através de seus próprios coletores de logs ou ferramentas de terceiros, conforme abaixo.

É importante notar 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 dos arquivos de logs seja configurada com sucesso.

SyslogAgent (Syslog Server), esta aplicação pode ser obtida via download pela URL: <http://syslogserver.com/>

- 1- Defina um IP remoto (Servidor que irá receber esses logs) 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 como guia de implementação PA-DSS do SiTef.



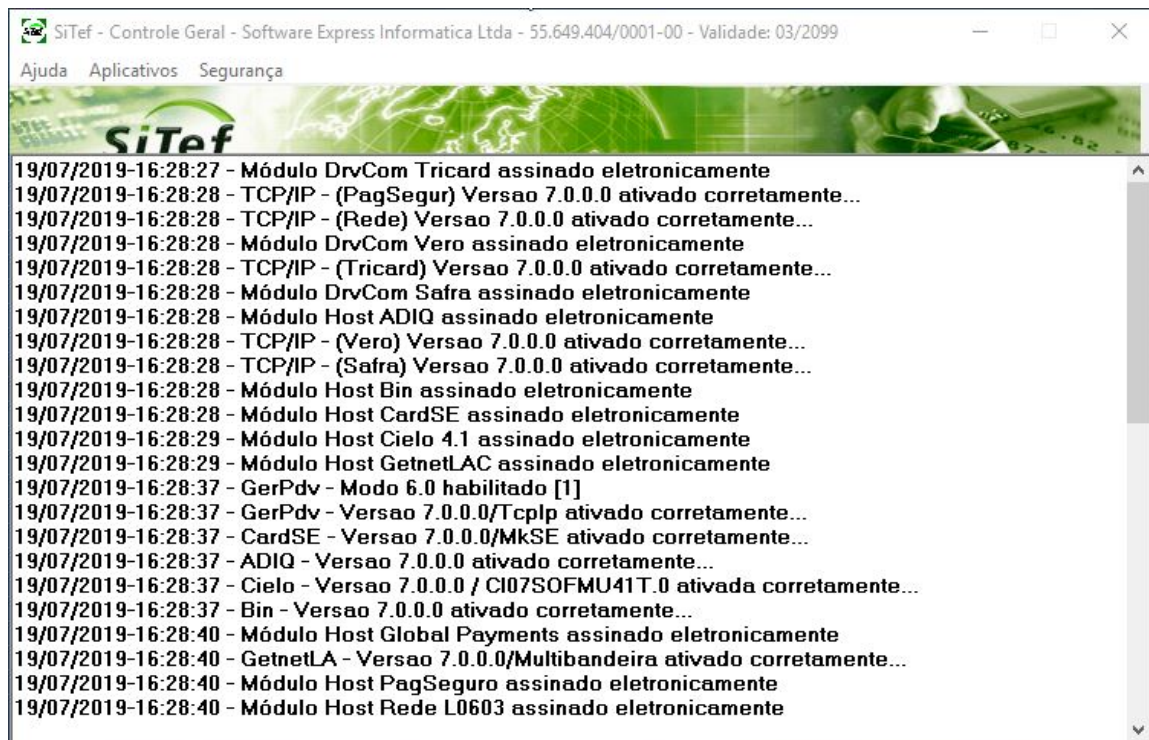
7. Contas de usuários

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 clients do SiTef (CliSiTef e Client SiTef Modular) não possuem interfaces, privilégios e contas para ser geridas.

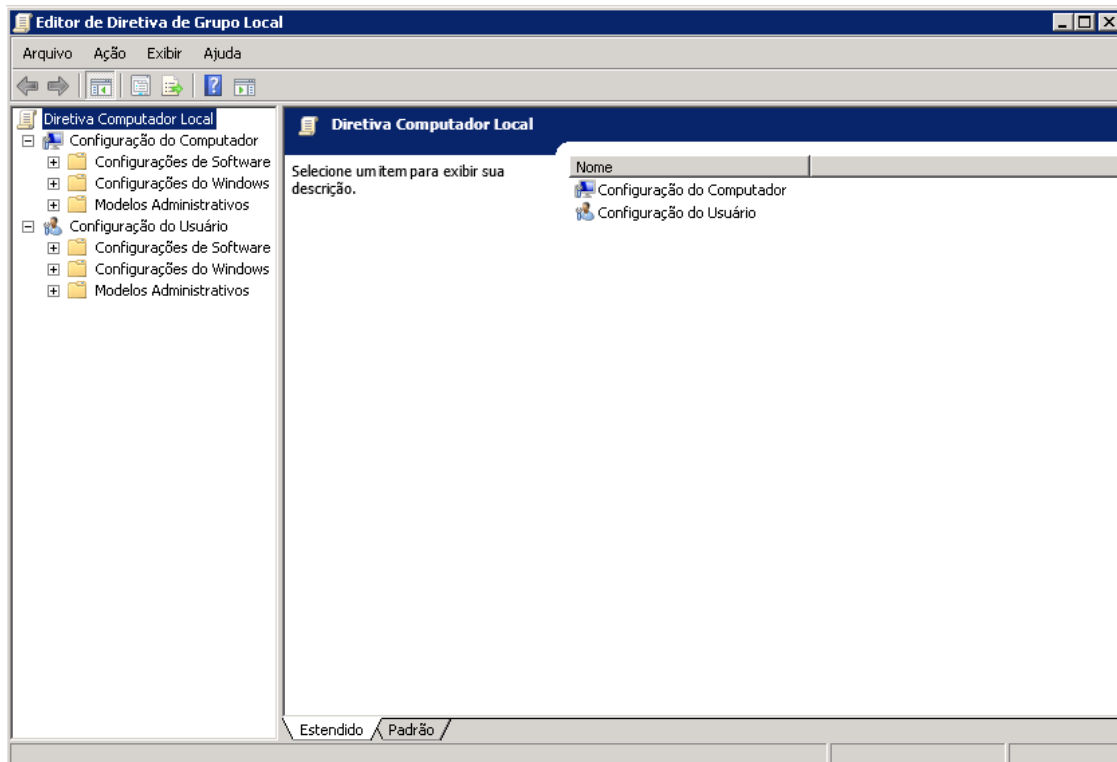
Para monitoração, o SiTef possui um aplicativo disponível “\\SiTef\\Aplic.win\\ControleGeralSitef.exe”, visível para todos os usuários, porém os menus estão somente disponíveis para aqueles pertencentes ao grupo “SiTef-Adm”.



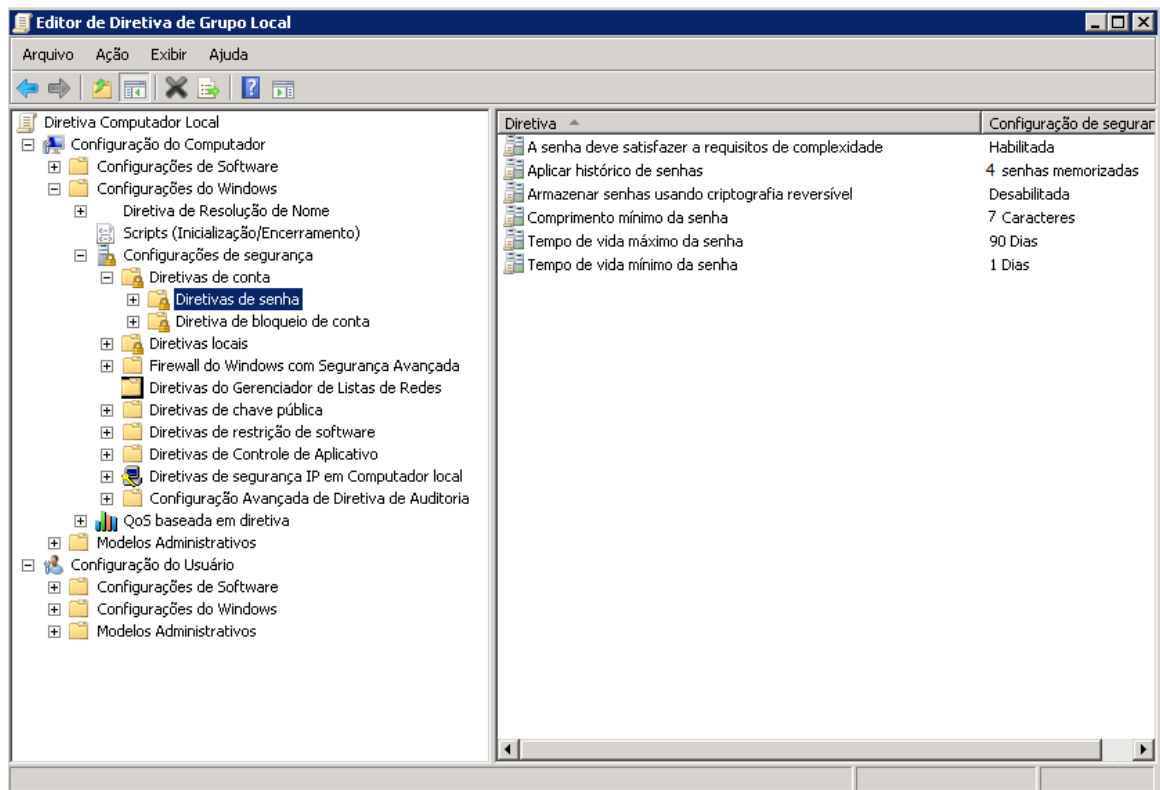
7.1. Configuração de Contas do Windows

Pelas regras PCI todas as contas de usuários do servidor Windows deverão seguir alguns requisitos de senha e bloqueio. Na sequência demonstramos como configurar estas características de senha e bloqueio.

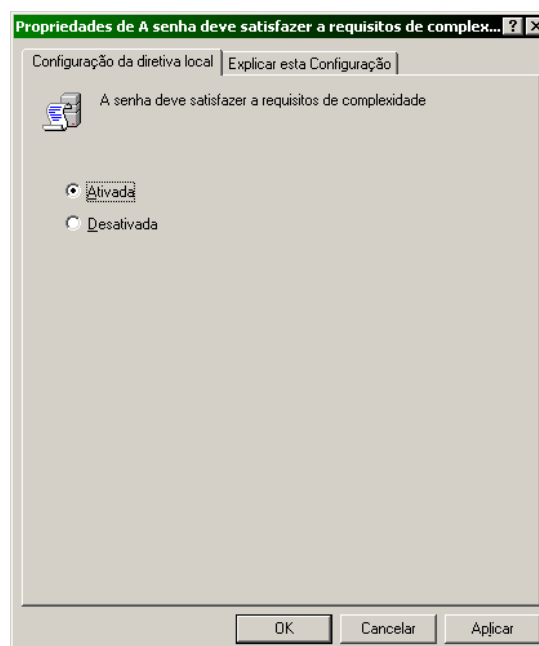
1. Clique no menu “Iniciar”, “Executar”, digite “gpedit.msc” e pressione “<enter>”;



2. Nas opções de tela à esquerda, selecione **Configuração do Computador**, **Configurações do Windows**, **Configurações de segurança**, **Diretivas de conta**, **Diretivas de senha**.



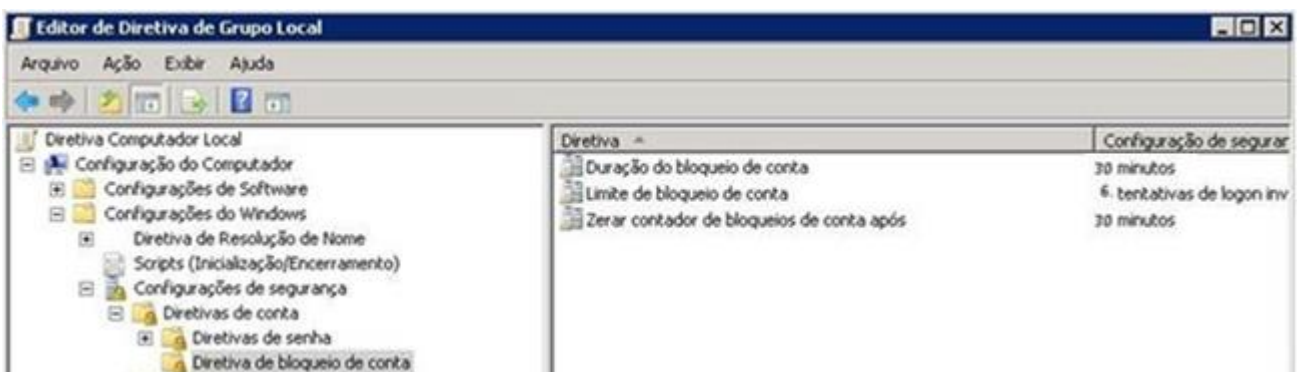
3. Clique na opção à esquerda “A senha deve satisfazer os requisitos de complexidade” e selecione a opção “Ativada” conforme tela abaixo:



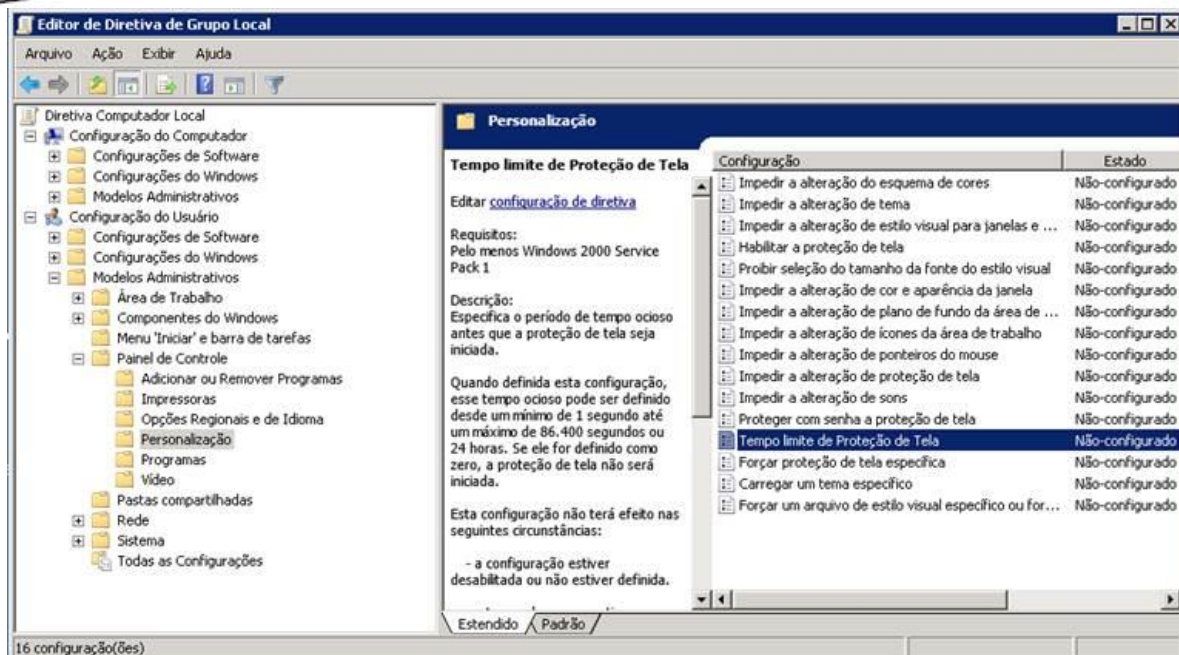
4. Realize este procedimento para todas as opções como segue abaixo:

Diretiva	Configuração de segurar
A senha deve satisfazer a requisitos de complexidade	Habilitada
Aplicar histórico de senhas	4 senhas memorizadas
Armazenar senhas usando criptografia reversível	Desabilitada
Comprimento mínimo da senha	7 Caracteres
Tempo de vida máximo da senha	90 Dias
Tempo de vida mínimo da senha	1 Dias

5. Clique nas opções de tela à esquerda “**Configuração do Computador, Configurações do Windows, Configurações de segurança, Diretivas de conta, Diretiva de bloqueio de conta**”



6. Clique na opção a esquerda “Diretiva de bloqueio de conta”
7. Clique na opção a direita “Limite de bloqueio de conta”;
Selecionar a opção: 6.
8. Clicar em OK
9. Selecionar a opção “Duração do bloqueio de conta”
Selecionar:30
10. Após passo anterior selecione a opção do lado esquerdo em: **Configurações do usuário, Modelos Administrativos. Painel de controle, Personalização**



11. Clique em “Habilitar a proteção de tela”
Selecione: Habilitado

12. Clique em “Forçar proteção de tela específica”
Selecione: Habilitado

13. Em “Nome do arquivo executável da Proteção de Tela”, coloque o caminho de um protetor de tela.

14. Clique em “Proteger com senha a proteção de tela”
Selecione: Habilitado

15. Clique em “Tempo limite de Proteção de Tela”
Selecione: Habilitado
Tempo de espera em segundos selecione 900.

8. 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” - “Limpa Chaves Criptografia” 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.

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 como guia de implementação PA-DSS do 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, *criptografias fortes* já fazem parte de seus requisitos de segurança (chaves de criptografias, como AES 128 bits ou superior, associada com os processos e procedimentos de administração de chave);
- ✓ Nenhum usuário possui acesso às chaves;
- ✓ Solicitar a troca das chaves anualmente conforme descrito acima;
- ✓ As chaves (modo criptografado) estão localizadas em: \\SiTef \\Etc\\ (uma chave é gerada para cada rede adquirente);
- ✓ O cliente deve evitar a substituição não autorizada dessas chaves criptografia que restringem a participação do grupo *SiTef-Admin*, que é o único grupo com privilégio para executar o procedimento para a substituição de chaves.

9. Metodologia de Versionamento SiTef

O SiTef utiliza um versionamento de acordo com o programa PA-DSS 3.2 como descrito abaixo:

- O código das versões é composto por quatro elementos: **xx.yy.zz.ttt**, cujos significados e conteúdo são descritos a seguir:

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 como guia de implementação PA-DSS do SiTef.

- **xx** – utilizado para indicar que é uma versão considerada de alto impacto, segundo as diretrizes do PA-DSS 3.2. São aceitos números de 0 a 99, sendo que o 0 à esquerda é omitido no caso de numerador inferior a 10 (O SiTef foi certificado PA-DSS a partir da versão 4);
 - **yy** – utilizado para indicar que é uma versão de baixo impacto, segundo diretrizes do PA-DSS 3.2. São aceitos números de 0 a 99, sendo que o zero à esquerda é omitido no caso de numerador inferior a 10;
 - **zz** – indica que a versão possui apenas alterações que respeitem as diretrizes do PA-DSS 3.2 como “No Impact” e que não afetam nenhum dos requerimentos do PA-DSS 3.2. Basicamente tratam de alterações em regras de negócio ou inclusão de novas funcionalidades, ou ainda, correções de problemas de regras de negócio de grande impacto; São aceitos números de 0 a 99, sendo que o zero à esquerda é omitido no caso de numerador inferior a 10;
 - **ttt** (0 a 999) – indica que a versão possui apenas alterações que respeitem as diretrizes do PA-DSS 3.2 como “No Impact” e que não afetam nenhum dos requerimentos do PA-DSS 3.2. Basicamente tratam de correções em regras de negócio de pequeno impacto. São aceitos números de 0 a 999, sendo que os zeros à esquerda são omitidos no caso de numerador inferior a 10.
- Os elementos são separados por ponto “.”;
 - Caso haja alteração dos elementos **xx** ou **yy** necessariamente a versão deve ser certificada;
 - Os elementos **zz** e **ttt** podem fazer uso de “wildcards”, desde que respeitadas as diretrizes do PA-DSS 3.2 como “No Impact”, e não utilizadas para mudanças de segurança de impacto.

10. Atualização dos Módulos

A atualização do SiTef, de seus módulos, bem como, de suas interfaces *clients* (CliSiTef e Client SiTef Modular) são disponibilizadas manualmente 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.

Tecnologias de acesso remoto não estão implementadas no SiTef. 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.

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

- a) Multi-fator de autenticação para acesso remoto. Utilizar VPN (TLS 1.2 ou IPSEC) com certificados individuais.
- b) Habilitar criptografia FORTE para o protocolo RDP, utilizado pelo aplicativo “*Conexão de área de trabalho remota*”;
- c) Implementar complexidade de senha, exigências de acordo com PCI-DSS;
- d) Permitir somente conexão de IP e *Mac address* conhecidos (específicos) ao servidor SiTef;
- e) Bloquear o terminal ocioso por mais de 15 minutos;
- f) Habilitar função de registro em log no servidor SiTef
- g) Os prestadores de serviços com acesso remoto às instalações do cliente, devem utilizar credenciais únicas de autenticação para cada cliente;
- h) Manter informações sobre quais exigências do PCI-DSS são geridas por cada prestador de serviço, e quais são geridas pelas entidades (instituições);
- i) 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 que afetam a segurança do cliente mantendo um ambiente com dados do titular do cartão.

11. Instruções gerais e informações

11.1. Definições de armazenamento de dados do portador do cartão

O SiTef está desenvolvido de forma a disponibilizar aos seus usuários apenas os dados permitidos. Outros dados como tarja magnética e código de segurança (CVC2, CVV2, CI) não devem ser armazenados. Vide tabela abaixo - Armazenagem dos dados *permitida/não permitida*:

		Elemento de dados	Armazenamento permitido	Converter dados armazenados ilegíveis conforme Requisito 3.4
Dados contáveis	Dados do portador do cartão	O número da conta principal (PAN)	Sim	Sim
		Nome do portador do cartão	Sim	Não
		Código de serviço	Sim	Não
		Data de vencimento	Sim	Não
	Dados de autenticação confidenciais ²	Dados de rastreamento completo ³	Não	Não armazenável conforme Requisito 3.2
		CAV2/CVC2/CVV2/CID ⁴	Não	Não armazenável conforme Requisito 3.2
		PIN/Bloco de PIN ⁵	Não	Não armazenável conforme Requisito 3.2

Os Requisitos 3.3 e 3.4 do PCI DSS aplicam-se apenas ao PAN. Se o PAN for armazenado com outros elementos dos dados do portador do cartão, somente o PAN deverá ser convertido como ilegível de acordo com o Requisito 3.4 do PCI DSS.

Dados de autenticação confidenciais não devem ser armazenados após a autorização, mesmo se forem criptografados. Isso se aplica mesmo onde não há PAN no ambiente. As organizações devem entrar em contato diretamente com seu adquirente ou empresa de pagamento para saber se é permitido armazenar o SAD antes da autorização, por quanto tempo e quaisquer requisitos de proteção e utilização.

(Referência: PCI-DSS 3.1)

onde:

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

Código de Serviço - Número de três ou quatro dígitos da tarja magnética que vem em seguida à data de validade do cartão de pagamento nos dados da tarja. Ele é usado para várias coisas, por exemplo, para definir atributos de serviço (*processamento de autorização*), diferenciar entre comércio nacional e internacional (*regras de intercâmbio*) e identificar restrições de uso (*serviços habilitados*).

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

Bloco de PIN (PIN Block) - é uma senha numérica secreta *criptografada* compartilhada entre o usuário e um sistema;

SAD (Dados de Autenticação Sensíveis) - Também chamado de dados de autenticação confidencial, são informações relacionadas à segurança de dados (Dados de trilha, Códigos de segurança e Bloco de Pin), utilizadas para autenticar portadores de cartões e/ou autorizar transações com cartão de pagamento.

- O armazenamento de cartões de forma temporária** e criptografada no SiTef ocorre apenas até o término da transação, depois disto qualquer dado será eliminado.
- Obrigatório aos clientes que necessitam armazenar cartões**, modalidade chamada “*Recorrente*” (por exemplo, assinatura de revistas, jornais,...etc), que o façam de forma protegida; utilizando chaves de criptografias, como AES 128 bits ou superior, associada com os processos e procedimentos de administração de chave.

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 como guia de implementação PA-DSS do SiTef.

c. Recomendações quanto à exibição dos dados:

- Nunca armazenar o código de segurança ou código de verificação do cartão;
- Ocultar parcialmente o PAN do cartão (número do cartão) ao exibi-lo em tela. Exibir conforme especificação das autorizadoras (6 primeiros e 4 últimos dígitos);
- Torne o PAN ilegível em qualquer local em que seja necessário armazená-lo;
- Nunca armazene a senha do cartão (PIN) ou Pin-Block (algoritmo de encriptação);
- Codificar informações pessoais; usando um algoritmo de criptografia forte, de acordo com a versão corrente do PCI-DSS, associada com os processos e procedimentos de administração de chave.

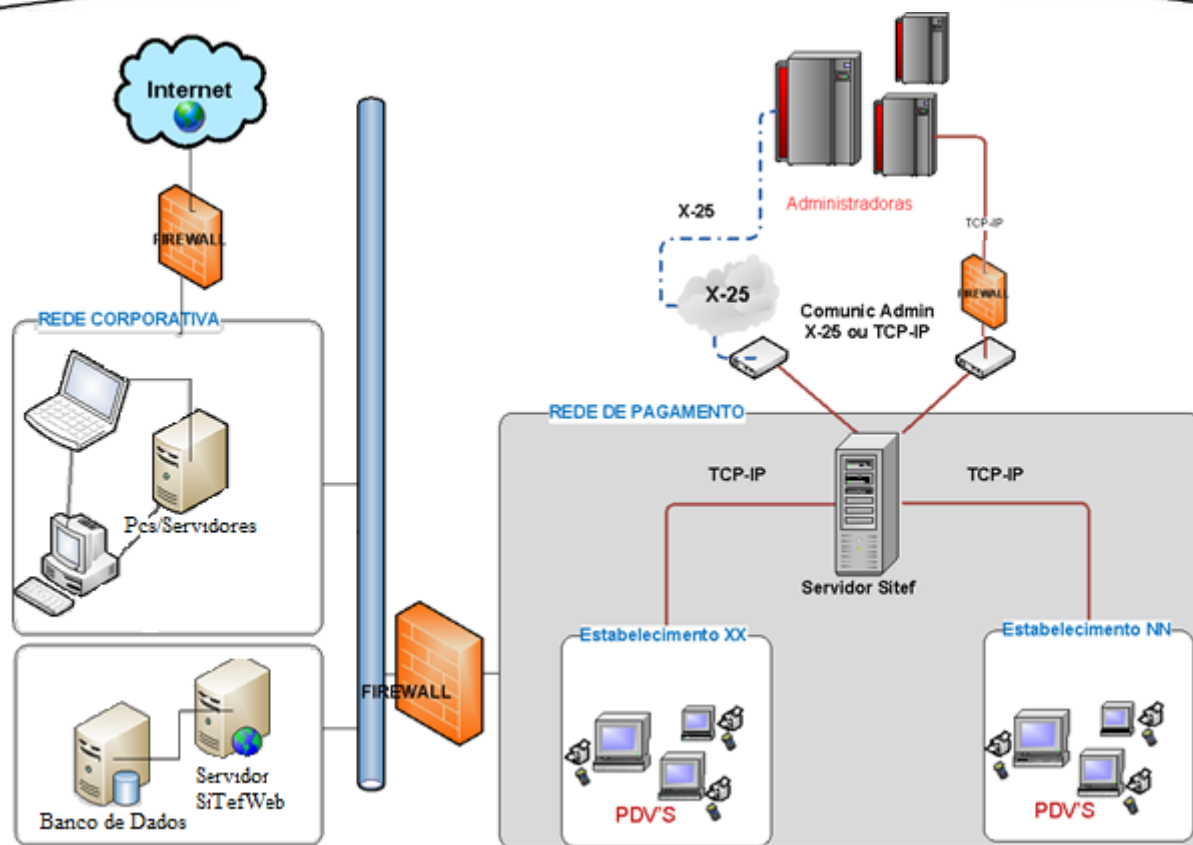
11.2. Backups

É altamente recomendável que o cliente execute backups tornando possível a recuperação dessas informações, sobre o histórico de transações. Para executar o backup é recomendado:

- 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. Armazenar em local seguro de preferência fora das instalações;
- e. Manter controle rigoroso sobre qualquer distribuição interna ou externa de qualquer tipo de mídia;
- f. Obter autorização da administração para o transporte das mídias, quando transportadas fora da área de segurança;
- g. Manter inventário rigoroso de todas as mídias.

11.3. Considerações relevantes para um Rede Segura

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, implementando um firewall entre as “Redes de pagamento” e todos os outros tipos de redes.

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.

- Sempre mude a senha padrão após a instalação de um sistema na rede;
- 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 (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);
- Desativar serviços e protocolos inseguros, bem como funcionalidades não utilizadas;
- Codifique todo acesso administrativo que não seja via console; Exemplo: Use tecnologias tais como SSH versão 2, VPN (utilizando algoritmo de criptografia AES 128 bits ou superior), ou TLS 1.2 para a administração baseada na web

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 como guia de implementação PA-DSS do SiTef.

e outro acesso administrativo. Para os sistemas operacionais Microsoft Windows ativar a criptografia FORTE para o protocolo RDP, usado pelo aplicativo "Remote Desktop Connection";

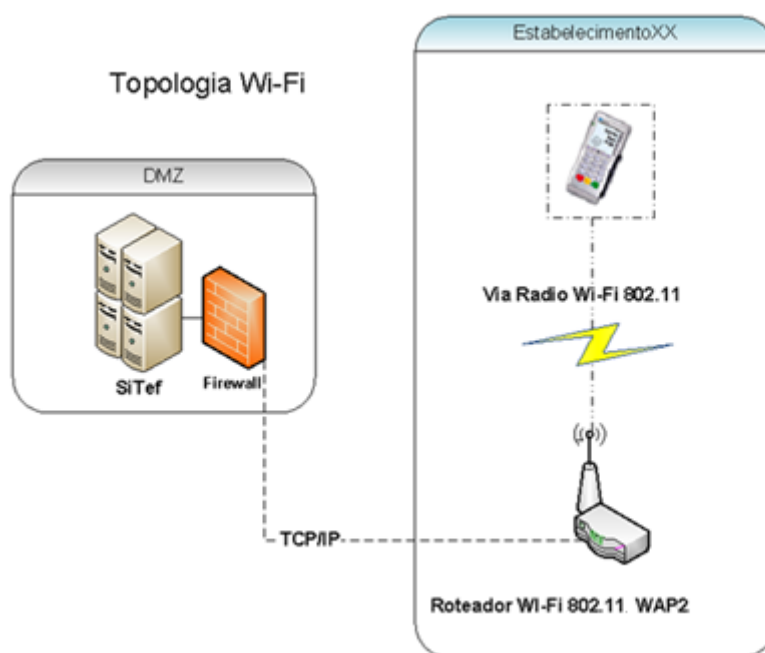
- e. Manter patches de segurança atualizados (em até 1 mês após o lançamento)
- f. Implementar processos para identificar vulnerabilidades de segurança;
- g. Implementar documentos para controle de mudanças (Descrição da mudança, criticidade, aprovações internas, liberação de acesso, documento de impacto, procedimentos de *Rollback* etc.);
- 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 acesso administrativo;
- i. Restringir o acesso aos dados do portador do cartão;
- j. Restringir o acesso de terceiros ao ambiente TEF (Limitar acesso);
- k. Criar ID único para cada usuário, inclusive para acessos remotos. (Senhas compartilhadas são proibidas);
- l. Verifique periodicamente sua rede à procura de pontos de vulnerabilidade, cabos ou pontos de rede aparentes (visíveis) que permitem pessoas não autorizadas ou inclusão de dispositivos em sua rede.

11.4. Considerações sobre Redes Wireless

O SiTef não possui como exigência a utilização de rede Wi-Fi (sem fio). Caso exista rede Wireless, os firewalls devem ser instalados nos perímetros das redes bloqueando o acesso ao ambiente de dados do titular do cartão. Se a rede sem fio é usada para fins comerciais (pela rede corporativa), também devem usar outros firewalls para controlar esse acesso, e uma segurança, mais rígida deve ser implementada utilizando pelo menos, as seguintes recomendações:

- a. Configurações **default** (padrão de fábrica) do dispositivo wireless devem ser alteradas:
 - i. Chaves de criptografia;
 - ii. Default **SNMP Community String** (vide glossário)
 - 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 WPA2 (Wi-Fi Protected Access) para a codificação e autenticação.
- c. Cifrar (**vide glossário**) com tecnologias WPA2, VPN IPSEC ou TLS 1.2 as transmissões para rede sem fios que trafegam dados do portador do cartão.
 - i. Usar somente em conjunto com tecnologias WPA2, VPN ou TLS 1.2;
 - 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.



Construa e mantenha um inventário de pontos *wireless* de acesso autorizados. Periodicamente realize a execução de uma varredura (scan) e inspeção física para detectar dispositivos sem fio não autorizados conectados em sua rede. Inclua aos procedimentos existentes, novos procedimentos de tratamento de incidentes para responder a incidentes quando novos pontos de acesso sem fio forem detectados.

11.5. Gerenciamento de Vulnerabilidades

- 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 e segurança;
- b. Implementar 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 relacionados ao ambiente TEF, arquivando estes acessos para ter um histórico de todas as pessoas que acessam e acessaram o ambiente do SiTef, PDVs e demais hardwares que compõe este 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 Antivírus 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), a menos que, especificamente autorizados pela Gerencia (a atribuição dessas permissões deve ser analisada caso a caso);
- e. Avaliar periodicamente 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 acesso 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 cartão de pagamento (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);
- i. Efetuar *scan* de vulnerabilidades periodicamente. Exemplos de alguns Software disponíveis para efetuar scan: NetBrute Scanner, Symantec Security Check, LANguard Network Scanner, Infiltrator Network Security Scanner;
- j. 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;
- k. Incluir sistemas de detecção de intrusão; existem vários softwares disponíveis conhecidos como IDS;
- l. Incluir software para validar a integridade de arquivos, há softwares disponíveis para esta validação;
- m. Realizar uma **avaliação de risco**, pelo menos, anualmente e após alterações significativas no ambiente.

11.6. Monitoração e armazenamento de logs

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

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 como guia de implementação PA-DSS do SiTef.

- v. Uso de mecanismos de identificação e autenticação
 - vi. Inicialização dos logs de auditoria
 - vii. Criação ou eliminação de objetos ao nível de sistema
Exemplo: 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:
- f. 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.;
- g. 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 TLS/IPSEC.
- h. Os arquivos de log não devem ser desabilitados, caso contrário, resultará em não-conformidade perante o PCI-DSS.

11.7. Plano de respostas 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 servidor;
- b. Teste o plano uma vez por ano;
- c. Designe funcionário 24x7 para responder a alertas;
- d. Faça treinamento apropriado;

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 como guia de implementação PA-DSS do SiTef.

- e. Incluir alertas originários de detecção de uma intrusão, penetração de sistema;
- f. Crie um plano de resposta a um incidente;
- g. 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;
- h. Implemente um processo para responder a quaisquer alertas gerados por mecanismos de detecção de mudança (Exemplo: Substituição de programas/executáveis, etc.);
- i. Pode-se efetuar uma replicação dos dados de um servidor de aplicação para outro servidor *Stand Alone* de modo *on-line*.

11.8. 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.

11.9. Contas de Usuário

- a. Contas devem ter 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 biometria;

- 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);
- 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. Bloquear a conta do usuário após não mais de 6 tentativas de login;
- 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 utilizadas) e, em seguida, desativar ou não utilizar essas contas.

11.10. Habilitando Serviços Necessários

Habilite os serviços necessários para que o SiTef funcione corretamente. Este funcionamento envolve toda parte de redes, protocolos, usuários, grupos, contas, notificações, conexões, drivers, horário do Windows, Acesso remoto, etc.

Exemplo: Windows 2016

- ✓ Agente de conexão de Rede
- ✓ Agente de eventos do sistema
- ✓ Agente de política IPsec
- ✓ Auxiliar IP
- ✓ Auxiliar NetBIOS TCP/IP
- ✓ Cliente de política de grupo
- ✓ Cliente de rastreamento de link distribuído
- ✓ Cliente DHCP
- ✓ Cliente DNS
- ✓ COM+ evento do sistema
- ✓ Coordenador de transações distribuídas
- ✓ Core messaging
- ✓ Detecção do hardware do Shell
- ✓ Estação de trabalho
- ✓ Gerenciador de conexões do Windows
- ✓ Gerenciador de credenciais
- ✓ Gerenciador de sessão local

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 como guia de implementação PA-DSS do SiTef.

- ✓ Gerenciador de usuários
- ✓ Gerente de contas de segurança
- ✓ Horário do Windows
- ✓ Informações sobre aplicativos
- ✓ Inicializador do processo de serviços DCOM
- ✓ Isolamento de chave CNG
- ✓ Ligar/Desligar
- ✓ Log de eventos do Windows
- ✓ Mapeador de ponto de extremidade RPC
- ✓ Módulos de criação de chave IKE e Auth IP do IPsec
- ✓ Plug and Play
- ✓ Reconhecimento de locais de rede
- ✓ RPC (Chamada de Procedimento Remoto)
- ✓ Server
- ✓ Serviço auxiliar de compatibilidade de programas
- ✓ Serviço da lista de redes
- ✓ Serviço de armazenagem
- ✓ Serviço de cache do Windows
- ✓ Serviço de compartilhamento de dados
- ✓ Serviço de descoberta de proxy da WEB do WinHTTP
- ✓ Serviço de gerenciador de licenças do Windows
- ✓ Serviço de Infraestrutura de tarefas de segundo plano
- ✓ Serviço de interface de repositório de rede
- ✓ Serviço de log para acesso de usuário
- ✓ Serviço de notificação de eventos do sistema
- ✓ Serviço de perfil de usuário
- ✓ Serviço de repositório de estado
- ✓ Serviço do sistema de notificação por PUSH do Windows
- ✓ Serviço de criptografia
- ✓ **SiTef - Solução Inteligente para Transação Eletrônica de Fundos**
- ✓ Testador de instrumentação de gerenciamento do Windows
- ✓ Windows driver foundation – Estrutura do driver de modo de usuário
- ✓ Windows remote management (WS – Management)

11.11. Sincronização de horário no servidor Windows Server 2016

É necessário possuir um servidor NTP (*Network Time Protocol*) disponível na rede.

11.12. Mantenha as políticas com Clientes e Integradores

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.

Quem distribui o Guia de Implementação?

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 como guia de implementação PA-DSS do SiTef.

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

Onde este assunto é tratado neste documento?

Este assunto é abordado no **item 11.8 – Políticas de Segurança** deste documento.

Qual a periodicidade com a qual o Guia de Implementação é atualizado?

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

12. Referencias do PA-DSS 3.2 no Guia de Implementação

Segue abaixo tabela com relacionamento entre os requerimentos do PA-DSS 3.2 e os tópicos desse documento.

PA-DSS 3.2 – Requerimentos	Tópico do Guia Implementação
Requerimento 1	4. Armazenamento de dados do Cliente (Rede Segura)
Requerimento 2	8. Chaves Internas de Criptografia
Requerimento 3	7. Conta de Usuários
Requerimento 4	6. Logs
Requerimento 5	9. Metodologia de Versionamento
Requerimento 6	11.4 Considerações sobre Rede Wireless
Requerimento 7	11.5 Gerenciamento de Vulnerabilidades
Requerimento 8	2. SiTef
Requerimento 9	3. Rede Segura
Requerimento 10	10. Atualização de Módulos
Requerimento 11	3. Rede Segura
Requerimento 12	3. Rede Segura
Requerimento 13	2. SiTef
Requerimento 14	11.12 Mantenha as políticas com Clientes e Integradores

13. 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
10/03/2011	1.5	Revisão Anual
14/03/2012	1.6	Revisão Anual
12/03/2013	1.7	Revisão Anual
17/02/2014	1.8	Atualização de acordo com as normas PCI-DSS 3.0
10/07/2015	1.9	Atualização segundo os padrões do Windows 2008 Server
08/12/2015	2.0	Inclusão do item 12 e alteração da criptografia PDV para AES 128 bits
04/01/2016	2.1	Inclusão da tabela de referência aos requerimentos do PA-DSS
04/01/2016	2.2	Corrigida a versão do TLS
04/01/2016	2.3	Alterada a versão do SiTef de 5.0.XX.XX para 6.1.XX.XX
14/01/2016	2.4	Correções ortográficas e de construção de frases
04/02/2016	2.5	Inclusão do Item: Implantar auditoria de segurança com políticas de Auditoria Central.
17/02/2016	2.6	Alterando algumas telas e efetuando correções ortográficas
10/05/2016	2.7	Correções ortográficas e de construção de frases
12/12/2016	2.8	Alterada a versão do SiTef de 6.1.XX.XX para 6.2.XX.XX
22/02/2018	2.9	Revisão Anual – PA-DSS 3.1
17/09/2019	3.0	Revisão Anual – PA-DSS 3.2 <ul style="list-style-type: none"> - Correções ortográficas e de construção de frases; - Alteração do termo duplo-fator para multi-fator descrito no item 10; - Alteração do título deste guia de SiTef 6.2.XX.XXX - PA-DSS 3.2 para SiTef 7.0.XX.XXX - PA-DSS 3.2; - Revisão do item 12 – Referencias do PA-DSS 3.2 no Guia de Implementação; - Inclusão no item 2 - SiTef instruções sobre PDV Android. - Alteração do protocolo mínimo para wi-fi, WPA2; - Alterações no item 6.2 - Auditoria de Segurança com políticas de Auditoria Central. - Item alterado de: Desabilitando Serviços Desnecessários para Habilitando Serviços Necessários. - Inclusão de clientes Android POS
02/03/2020	3.1	<ul style="list-style-type: none"> - Retirada do S.O Windows 7 devido ao fim da validade deste sistema operacional - item 2.1 - SiTef e Clients - Versões e Sistemas Operacionais; - Inclusão no glossário dos termos SIEM e <i>hardening</i>

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 como guia de implementação PA-DSS do SiTef.

14. Glossário

A

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.

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.

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.

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 como guia de implementação PA-DSS do SiTef.

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.

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.

Hardening

É um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

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.

Invasão

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

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.

SIEM

SIEM (Security Information and Event Management) – Uma solução SIEM permite que os eventos gerados por diversas aplicações de segurança (tais como firewalls, proxies, sistemas de prevenção a intrusão (IPS) e antivírus sejam coletados, normalizados, armazenados e correlacionados; o que possibilita uma rápida identificação e resposta aos incidentes.

Enquanto ferramentas SEM oferecem monitoramento em tempo real dos eventos de segurança, coletando e agregando os dados (com resposta automática em alguns casos); uma ferramenta SIM oferece análise histórica dos eventos de segurança, também coletando e correlacionando os eventos, porém não em tempo real; o que permite consultas mais complexas ao repositório.

As soluções SIEM combinam os recursos oferecidos em ambas as tecnologias (SIM e SEM)

SSH

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 "syslog", "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 infraestrutura. 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.

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 uma 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.

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.