



Guia de Administração

Versão 1.01 (01 abr 2009)

CONTEÚDO

Sobre este documento.....	3
Escopo.....	3
Público.....	3
Referências	3
Avisos.....	3
Histórico	4
Introdução	5
Arquitetura	6
Operação dos Terminais Virtuais	9
Operação no Servidor Pay&Go	10
Operação no Checkout.....	11
Modalidade de Pagamento	12
Modalidade Administrativa	12
Gerenciamento Avançado	13
Consulta de transações	13
Exportação manual de transações	15
Exportação automática de transações	16
Resolução de pendências.....	17
Limpeza de registros	18
Gerenciamento Remoto.....	19
Troca de chaves.....	21
Conformidade e Segurança	22
Uso do PIN-pad.....	22
Dados históricos.....	22
Coleta de arquivos	22
Configuração de contas de usuário	23
Monitoração.....	23
Atualização de sistemas e equipamentos.....	24
Configuração de equipamentos e rede	24
Configuração de redes sem fio	25
Acesso remoto	25
Outros requerimentos	25

SOBRE ESTE DOCUMENTO

Escopo

O propósito deste documento é conter todas as informações necessárias para a operação e manutenção da solução **Pay&Go**, considerando:

- Funcionalidades do módulo **Servidor Pay&Go**;
- Boas práticas referentes à configuração do sistema e do ambiente no qual este opera.

Público

Este documento se destina a:

- Funcionários do estabelecimento comercial onde o sistema é instalado, e que sejam responsáveis:
 - pela operação do sistema **Servidor Pay&Go**;
 - pela administração da rede local do estabelecimento;
- Técnicos responsáveis pela instalação do sistema.

Referências

Outros documentos referenciados por este documento, ou que o complementem:

- "Guia de Referência Pay&Go": informações referentes à operação do sistema no checkout.

Avisos

As informações contidas neste documento estão sujeitas a alteração sem prévio aviso.

Pay&Go é uma marca registrada da SETIS Automação e Sistemas Ltda.

Microsoft e *Windows* são marcas registradas da Microsoft Corporation.

© 2008 SETIS Automação e Sistemas Ltda. Todos os direitos reservados.

HISTÓRICO

v1.00 (30 nov 2008)

Primeira versão oficial, revisada durante o processo PABP-DSS.

v1.01 (01 abr 2009)

- Inclusão: seção "Uso do PIN-pad".
- Revisão (ajustes pontuais).

INTRODUÇÃO

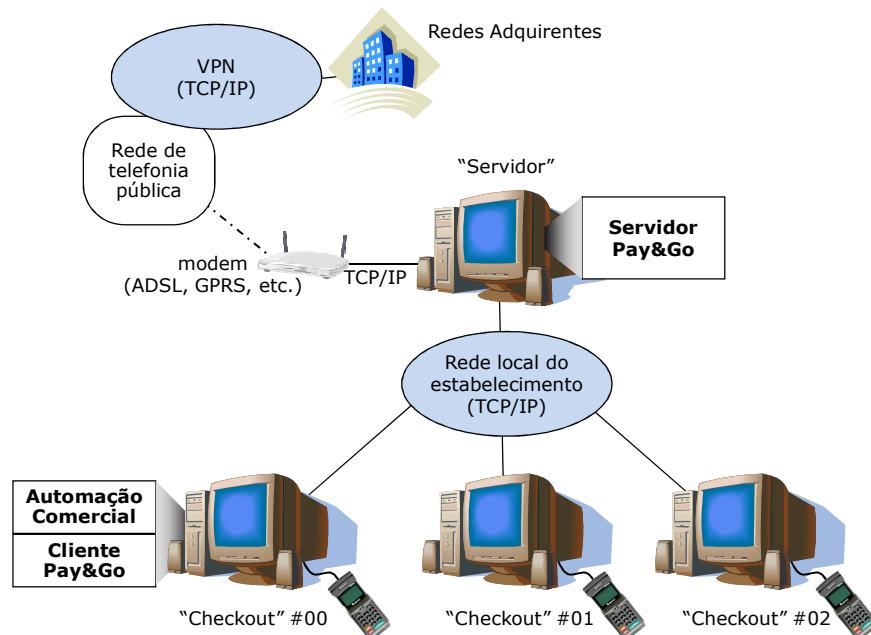
O **Pay&Go** é um produto destinado a estabelecimentos comerciais dos diversos segmentos do mercado brasileiro, para realização de transações eletrônicas de pagamento de alta performance através da tecnologia TCP/IP.

Glossário:

Checkout ou PDV	Terminal de caixa utilizado para pagamento de mercadorias e serviços comercializados pelo estabelecimento. O checkout usualmente possui uma aplicação de Automação comercial , responsável pela captura das informações dos produtos sendo adquiridos, controle de uma impressora fiscal e registro dos meios de pagamento.
Rede adquirente	Empresa responsável por prover o serviço de captura de transações eletrônicas (seja de cartão de crédito/débito ou outro meio de pagamento). Visanet, Redecard, American Express, Hipercard e Banrisul são exemplos de Redes adquirentes do mercado brasileiro.
Cliente	Pessoa física ou jurídica adquirindo mercadorias ou serviços do estabelecimento comercial, responsável pelo pagamento destas e portador de um cartão ou outro meio de pagamento. A única exceção a esta definição é o uso do nome "Cliente Pay&Go", que designa o módulo aplicativo do Pay&Go instalado no checkout.
PIN-pad	Equipamento seguro certificado pelas Redes adquirentes e destinado à leitura de cartão com tarja magnética, captura da senha do cliente (PIN = <i>Personal Identification Number</i>) e processamento de cartões com <i>chip</i> .
TCP/IP	TCP/IP designa um conjunto de protocolos de comunicação entre computadores em rede. As duas camadas TCP (<i>Transmission Control Protocol</i>) e IP (<i>Internet Protocol</i>) são utilizadas por camadas de mais alto nível, que dependem da aplicação, e por outro lado se utilizam de camadas de mais baixo nível, que dependem do meio físico utilizado (seja Ethernet, GPRS, ADSL, linha discada ou outro) para a comunicação.

ARQUITETURA

Para a correta administração da solução **Pay&Go**, é fundamental o conhecimento da sua arquitetura, ilustrada na figura a seguir:

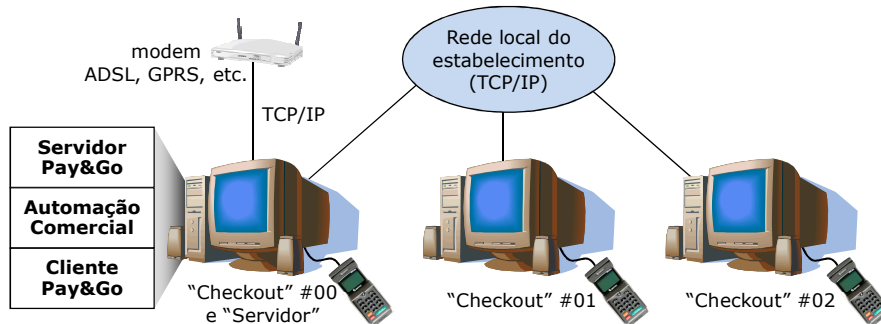


O estabelecimento deve destinar uma máquina com Microsoft Windows para instalação do módulo principal da solução, o **Servidor Pay&Go**.

Os checkouts do estabelecimento devem estar conectados ao "Servidor" através de uma rede local Ethernet configurada com protocolo TCP/IP. Cada checkout deve contar com:

- Um aplicativo de Automação comercial, responsável por gerenciar o processo de venda;
- O módulo **Cliente Pay&Go**, acionado pela Automação comercial para efetuar o pagamento eletrônico de todo ou parte do valor da venda, e responsável pela comunicação com o **Servidor Pay&Go**.
- Um PIN-pad conectado a uma porta serial ou USB;
- Uma impressora, normalmente fiscal, gerenciada pela Automação comercial e utilizada para imprimir as duas vias (uma para o estabelecimento, outra para o cliente) do comprovante de pagamento eletrônico.

Pode-se também adotar uma arquitetura alternativa onde um dos checkouts faz o papel de "Servidor", conforme figura a seguir:



Esta arquitetura é a mais conveniente para os estabelecimentos que possuem poucos ou um único checkout.

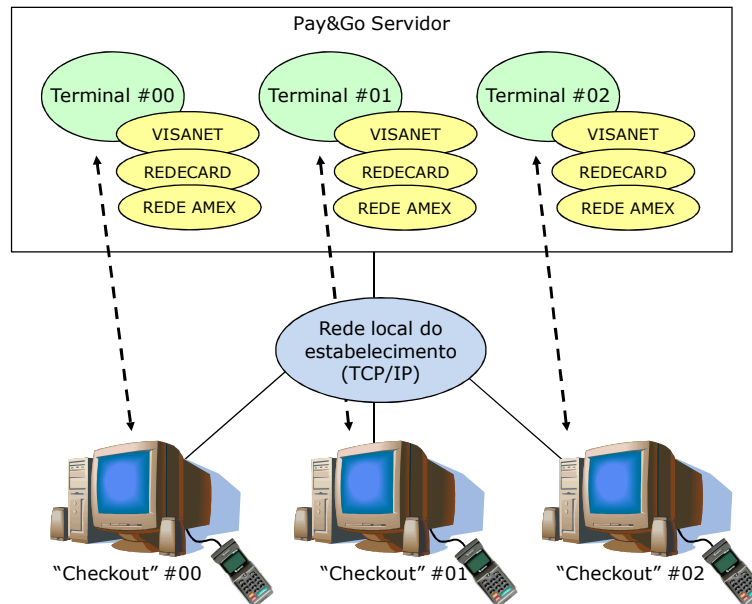
IMPORTANTE:

O aplicativo **Servidor Pay&Go** requer uma versão 32 bits do sistema operacional Microsoft Windows para funcionar e é compatível com qualquer uma delas. No entanto, como requerimento de segurança (mais informações no capítulo "Conformidade e Segurança", página 22), somente podem ser utilizadas versões ainda suportadas pela Microsoft (ou seja, que recebem atualizações de segurança).

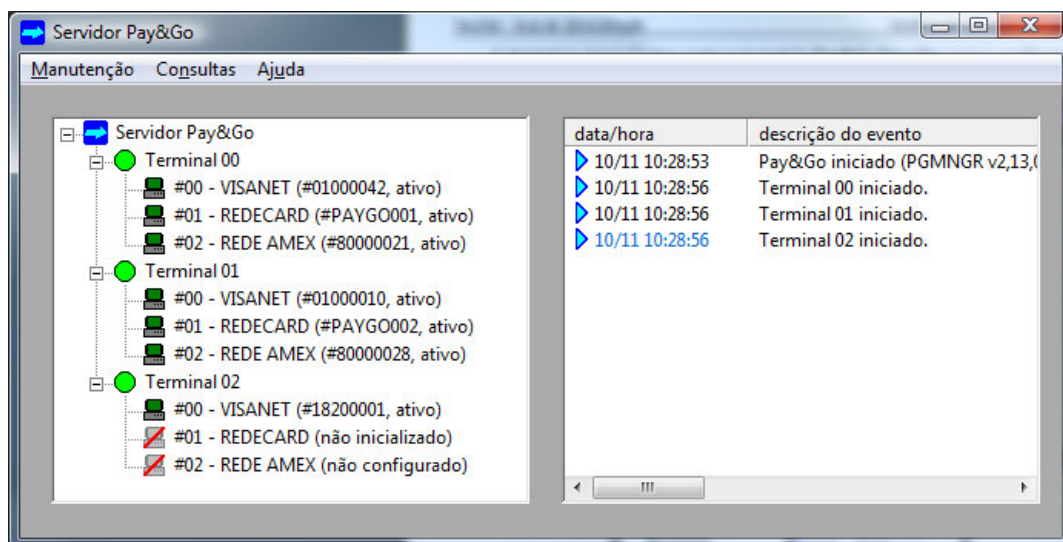
Para o checkout, várias plataformas são suportadas. No entanto, as mesmas regras do equipamento "Servidor" acima se aplicam para o sistema operacional Microsoft Windows.

A aplicação **Servidor Pay&Go** é um sistema multi-tarefa que cria um processo paralelo independente para cada checkout, chamado de "terminal virtual". Todo o processamento do **Pay&Go** é feito pelos "terminais virtuais" no Servidor, sendo que os checkouts apenas proporcionam a interface com o usuário, além de um meio de comunicação entre o PIN-pad e seu respectivo "terminal virtual".

IMPORTANTE: Cada terminal virtual se comporta como um terminal de pagamento único e distinto para cada uma das Redes adquirentes em operação. Por exemplo, em um estabelecimento com três checkouts habilitados a operar com Visanet, Redecard e a Rede Amex, para todos os efeitos, existem nove terminais de pagamento, conforme figura abaixo:



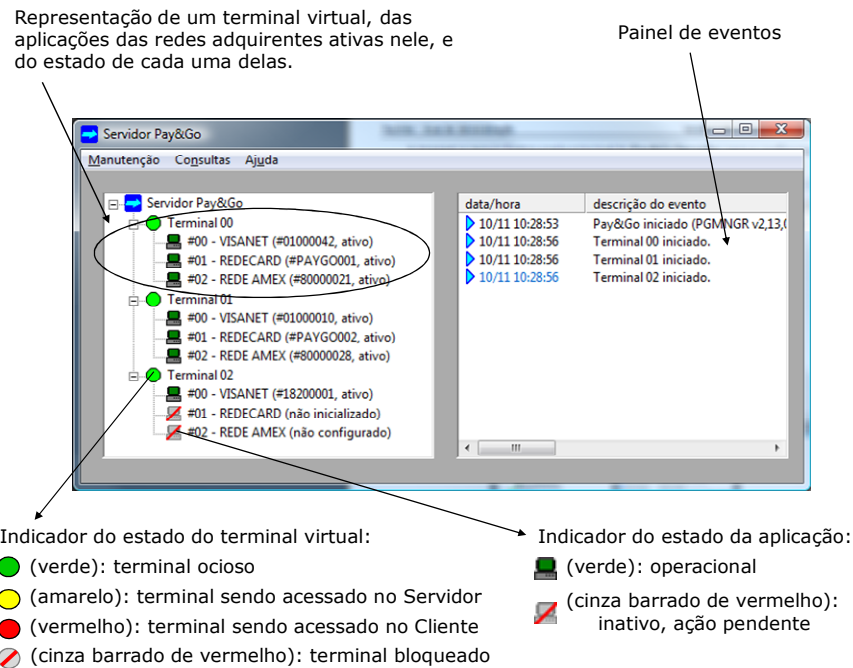
A imagem a seguir ilustra a tela principal do **Servidor Pay&Go** para a configuração acima, onde três checkouts estão ativos no estabelecimento:



OPERAÇÃO DOS TERMINAIS VIRTUAIS

Este capítulo descreve a operação dos terminais virtuais do **Pay&Go**.

A ilustração a seguir mostra a tela principal do **Servidor Pay&Go** e o significado dos seus componentes:



Os terminais virtuais podem ser acessados de duas maneiras:

- Diretamente no **Servidor Pay&Go**; ou
- No checkout, com iniciativa da Automação e uso do **Cliente Pay&Go**.

Operação no Servidor Pay&Go

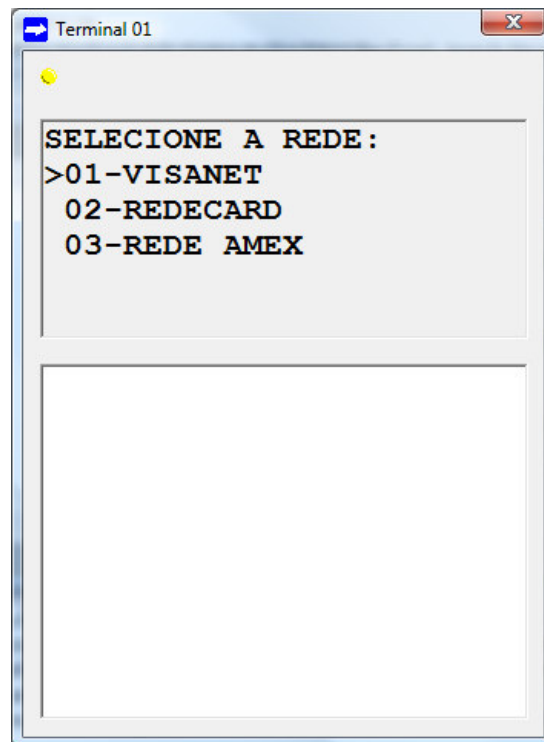
A operação dos terminais virtuais diretamente pelo **Servidor Pay&Go** é limitada a operações administrativas que não requeiram o uso do PIN-pad, como por exemplo:

- Alteração de configuração;
- Inicialização (dependendo da Rede adquirente);
- Fechamento de lote.

Para iniciar uma operação em modo local a partir do **Servidor Pay&Go**:

- Selecionar o terminal virtual desejado (clique uma vez no texto "Terminal XX");
- Pressionar a tecla [Enter];
- Pressionar qualquer tecla.

Uma janela aparecerá, permitindo operar o terminal virtual normalmente através do teclado, como seria feito no checkout (ver a seção "Operação no Checkout", página 11):



Observações:

- Após a seleção da Rede adquirente, o menu de funções administrativas correspondente será apresentado.
- Caso a função realizada gere um comprovante, este poderá ser visualizado na parte inferior da janela do terminal virtual, porém não será impresso.
- Enquanto o terminal virtual é usado em modo local, este não pode ser acessado pelo checkout. Esta situação é caracterizada pela cor amarela do identificador do estado do terminal virtual no **Servidor Pay&Go**, e pela mensagem "TERMINAL OCUPADO" no **Cliente Pay&Go**.

Operação no Checkout

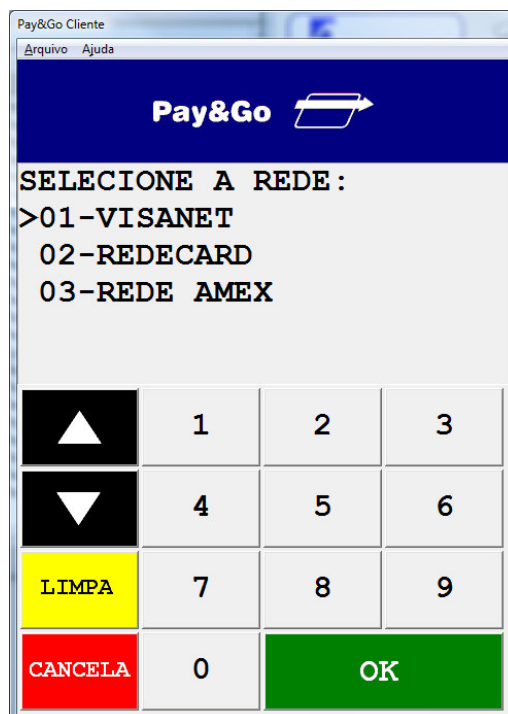
A operação no checkout é sempre iniciada pela Automação comercial, e realizada através do **Cliente Pay&Go**.¹

No momento em que uma operação é iniciada, uma tela é apresentada para interação com o terminal virtual através do teclado do checkout:

- Teclas numéricas e alfanuméricas permitem a entrada de dados ou a seleção direta de uma opção de menu;
- As setas permitem a navegação nos menus de opções;
- A tecla [Enter] permite confirmar uma escolha, um aviso, ou finalizar uma entrada de dados;
- A tecla [Backspace] apaga o último caractere durante uma entrada de dados;
- A tecla [Esc] interrompe a operação em curso.

Caso uma confirmação ou uma entrada de dados deva ser realizada pelo cliente, não pelo operador do estabelecimento, o PIN-pad será automaticamente acionado.

A primeira tela apresentada após o início de uma operação é um menu com os nomes das Redes adquirentes habilitadas no estabelecimento. Após seleção da aplicação desejada, o fluxo de telas apresentado é específico e de acordo com as especificações desta. Um operador acostumado a operar os equipamentos "terminais POS" das Redes adquirentes perceberá que o fluxo de telas é muito similar ao do **Pay&Go**.



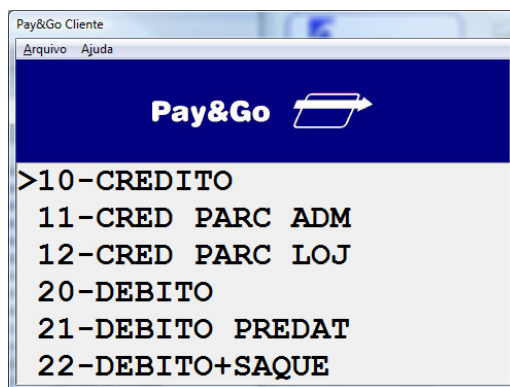
¹ Para a especificação da interface entre a Automação comercial e o **Cliente Pay&Go**, consulte a NTK Solutions Ltda. (<http://www.ntk.com.br>).

No acionamento do **Pay&Go** pela Automação comercial, uma de duas modalidades é selecionada:

- Modalidade de pagamento;
- Modalidade administrativa.

Modalidade de Pagamento

A modalidade de pagamento é utilizada pela Automação comercial na finalização do cupom fiscal, quando é selecionada a forma de pagamento eletrônico. Nesta situação, o **Pay&Go** somente apresenta as funções do terminal virtual que correspondem ao pagamento de mercadorias ou serviços para a Rede adquirente selecionada, por exemplo:



Na modalidade de pagamento, quando a operação é bem sucedida, dois comprovantes não fiscais são emitidos (uma via para o cliente, outra para o estabelecimento), e devem ser vinculados ao cupom fiscal da venda.

Modalidade Administrativa

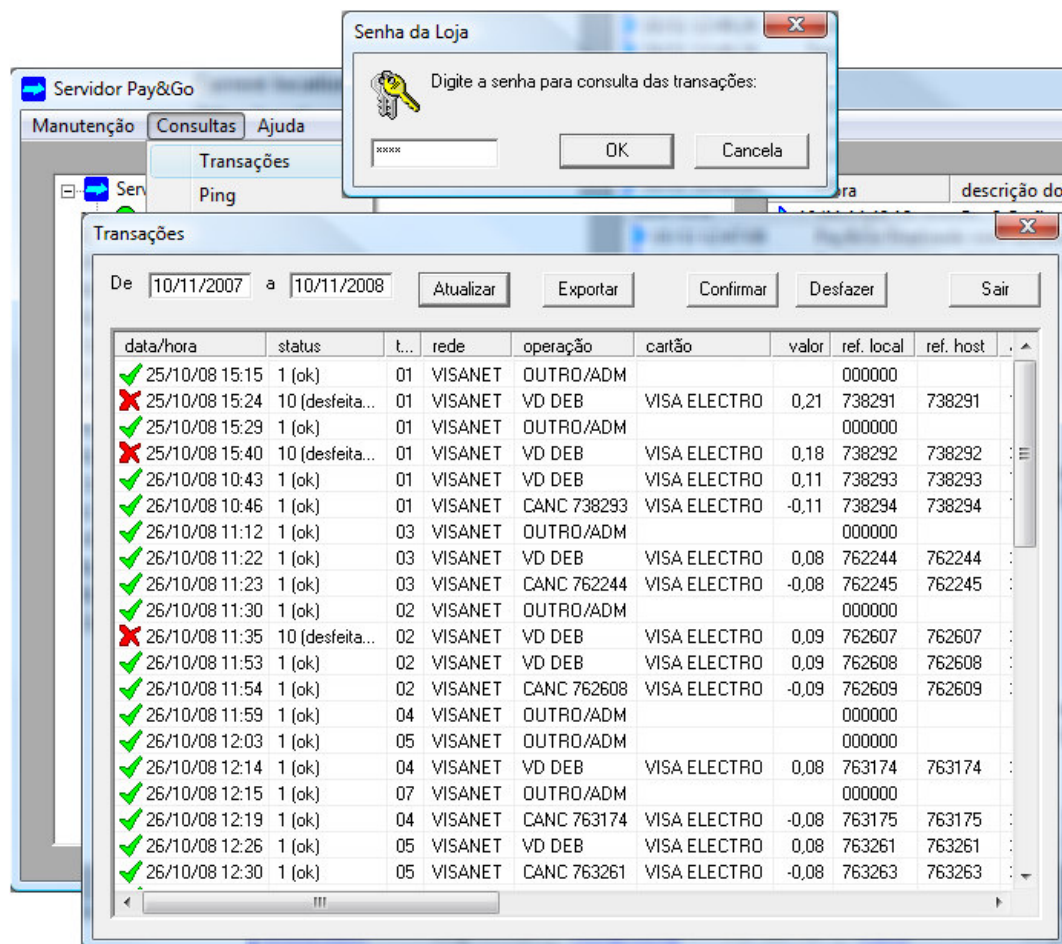
A modalidade administrativa permite acessar todas as funções do terminal virtual definidas por cada Rede adquirente, exceto as destinadas ao pagamento de mercadorias, por exemplo:

- Configuração de parâmetros;
- Inicialização (*download* de parâmetros);
- Pré-autorização;
- Consultas (de saldo, cheque, informações de financiamento, etc.);
- Cancelamento ou Estorno;
- Pagamento de conta;
- Fechamento de lote;
- Envio de transações pendentes;
- Reimpressão de comprovante;
- Emissão de relatórios;
- etc.

GERENCIAMENTO AVANÇADO

Consulta de transações

As transações efetuadas através do **Pay&Go** ficam registradas no **Servidor Pay&Go** para consulta a qualquer momento. Isso pode ser feito através da opção "Transações" do menu "Consultas", após a digitação da Senha da Loja (senha padrão: "**1111**"):



Como padrão, a tela de consulta apresenta somente as transações efetuadas na data corrente. Caso seja necessário consultar transações de outros períodos, podem ser informadas as datas inicial e final no canto superior esquerdo da tela, validando-as através do botão "Atualizar".












As seguintes transações são registradas para consulta:

- Transações de pagamento bem sucedidas (aprovadas);
- Transações administrativas bem sucedidas e que tenha gerado um comprovante.

Para cada transação registrada, as seguintes informações estão disponíveis:

- **data/hora:** data e hora da transação, conforme impresso no comprovante (horário da Rede adquirente). O ícone à esquerda indica se a transação é válida, se foi anulada ou se está pendente de confirmação (ver item "status" a seguir);

- **status:** indica o status da transação, se esta é válida ou se foi anulada por algum motivo específico. Os seguintes status estão previstos:

 0	Resultado final da transação ainda pendente de confirmação pelo checkout.
 1	Transação confirmada pela Automação comercial.
 2	Transação confirmada automaticamente (realizada em modo local, no Servidor Pay&Go).
 3	Transação confirmada manualmente (ver "Resolução de pendências", página 17).
 4	Transação desfeita pela Automação comercial, provavelmente por problemas de impressão.
 5	Transação desfeita manualmente (ver "Resolução de pendências", página 17).
 6	Transação desfeita por erro interno ao Pay&Go.
 7	Transação confirmada manualmente, porém ainda não processada.
 8	Transação desfeita manualmente, porém ainda não processada.
 9	Transação confirmada manualmente no Cliente Pay&Go após tentativa de desfazimento pela Automação.
 10	Transação desfeita manualmente no Cliente Pay&Go após tentativa de desfazimento pela Automação.

- **term.:** número (índice iniciado em 00) do terminal virtual que efetuou a transação.
- **rede:** nome da Rede adquirente através da qual foi efetuada a transação.
- **operação:** descrição da operação efetuada, de acordo com a seguinte nomenclatura:

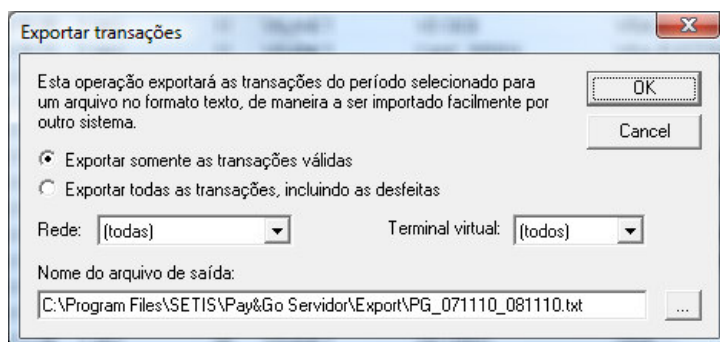
VD CRED	Venda com cartão de crédito, à vista.
VD CRED xP ADM	Venda com cartão de crédito, parcelada pela administradora em 'x' parcelas.
VD CRED xP LOJ	Venda com cartão de crédito, parcelada pelo estabelecimento em 'x' parcelas.
VD DEB	Venda com cartão de débito, à vista.
VD DEB PRE dd-mm-aa	Venda com cartão de débito, pré-datada para o dia 'dd-mm-aa'.
VD VOUCH	Venda com cartão voucher/convênio.
PREAUT	Pré-autorização com cartão de crédito.
CONSULTA	Consulta.
CANC dddddd	Cancelamento da transação de número de documento 'dddddd'.
CANC PREAUT dddddd	Cancelamento da transação de pré-autorização de número de documento 'dddddd'.
FECHAMENTO	Fechamento/finalização.
OUTRO/ADM	Outra operação administrativa que gerou comprovante.

- **cartão:** nome do emissor do cartão ou informação similar fornecida pela aplicação da Rede adquirente.
- **valor:** valor da transação (negativo no caso de um cancelamento).
- **ref. local:** identificador da transação para o Pay&Go (impresso no comprovante).
- **ref. host:** identificador da transação para a Rede adquirente (impresso no comprovante).
- **autoriz.:** código de autorização para a transação, recebido da Rede adquirente.
- **num. lógico:** número lógico do terminal virtual (referência da Rede adquirente).
- **cód. estab.:** código do estabelecimento para a Rede adquirente.
- **mensagem:** descrição do resultado da transação (por exemplo "APROVADA 123456")

- **doc. fiscal:** número do documento fiscal informado pela Automação.
- **dados adic.:** dados adicionais informados pela Automação.

Exportação manual de transações

A tela de Consulta de transações possui um botão “Exportar” que pode ser utilizado para exportar as transações visualizadas. Algumas opções são apresentadas no momento da exportação:



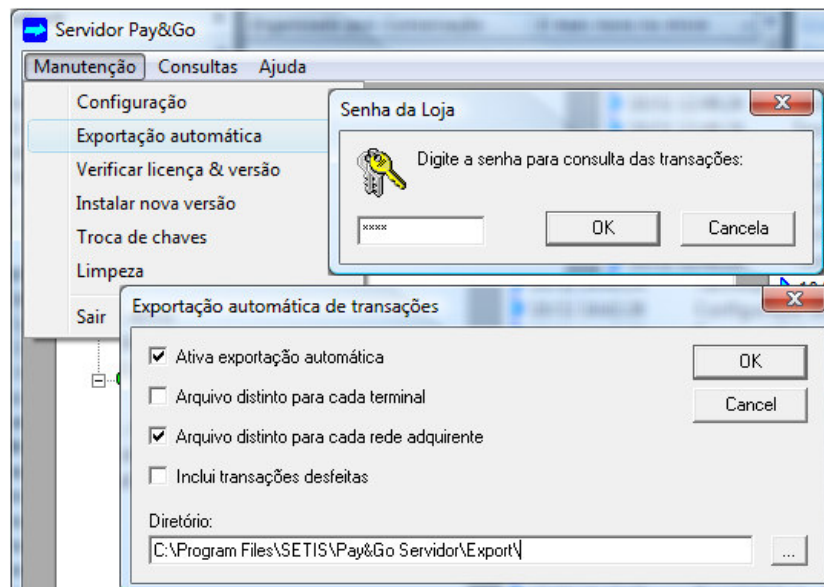
Normalmente, somente as transações válidas são relevantes para o estabelecimento, porém o **Servidor Pay&Go** permite a exportação de todas as transações, incluindo as desfeitas, para o caso de depuração do sistema ou questões envolvendo liquidação indevida. Pode-se também optar por exportar as transações de todas as Redes adquirentes ou de uma Rede adquirente específica, e também de todos os terminais virtuais ou de um terminal virtual específico.

O **Servidor Pay&Go** sempre sugere um nome do arquivo gerado com base nas datas de início e fim do período, porém este pode ser alterado pelo operador.

O arquivo é gerado no formato texto, contendo exatamente as mesmas informações da tela de consulta, com uma transação por linha, sendo que os campos são separados por tabulações (caractere TAB). Este arquivo pode ser importado diretamente por qualquer sistema de banco de dados ou de planilha eletrônica (como o Microsoft Excel).

Exportação automática de transações

O **Pay&Go** pode também ser programado para exportar automaticamente todas as transações realizadas. Esta funcionalidade pode ser configurada através da opção "Exportação automática" do menu "Manutenção", após a digitação da Senha da Loja (senha padrão: "**1111**"):



Com a funcionalidade ativa, o **Servidor Pay&Go** cria automaticamente e diariamente às 02:00 (ou no momento em que o **Servidor Pay&Go** for reiniciado caso não esteja sendo executado neste horário) um ou mais arquivos contendo as transações realizadas durante o dia anterior (de 00:00 a 23:59).

O formato dos arquivos gerados é exatamente o mesmo da exportação manual (descrito página 15).

O nome dos arquivos gerados respeita a nomenclatura a seguir, dependendo das configurações da exportação automática:

- **PG_aaaammdd_idididid.txt;**
- **PG_aaaammdd_idididid_tpp.txt;**
- **PG_aaaammdd_idididid_rede.txt;** ou
- **PG_aaaammdd_idididid_tpp_rede.txt.**

Onde:

- 'aaaammdd' é a data das transações exportadas;
- 'idididid' é o identificador da instalação do **Servidor Pay&Go** (ver "Gerenciamento Remoto", página 19), com 8 dígitos;
- 'pp' é o número (índice iniciado em 00) do terminal virtual, com 2 dígitos;
- 'rede' é o nome da Rede adquirente ("VISANET", "REDECARD", etc.).

Observações:

- Para facilitar a importação automática dos arquivos por outro sistema, todos os arquivos são gerados diariamente, mesmo que não contenham nenhum registro.

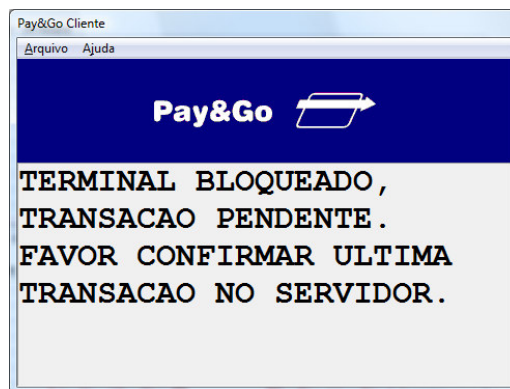
- Ao ser ativada a funcionalidade pela primeira vez, serão automaticamente gerados os arquivos referentes a todas as transações já realizadas, até o dia anterior à ativação.

Resolução de pendências

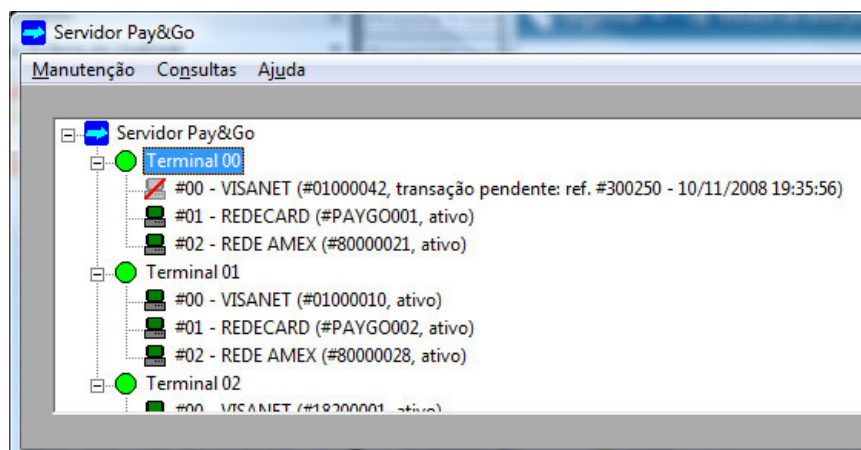
Ao final de cada transação, a Automação comercial é responsável por indicar o status final desta ou seja, se foi finalizada com sucesso ou se deve ser desfeita, o que ocorre geralmente por uma falha ao registrar o pagamento na impressora fiscal.

Com o objetivo de garantir a integridade transacional, importante tanto para o estabelecimento como para o cliente, o **Pay&Go** não permite que nenhuma transação possa ser iniciada com um terminal virtual caso o status final da transação anterior não tenha sido informado para este terminal.

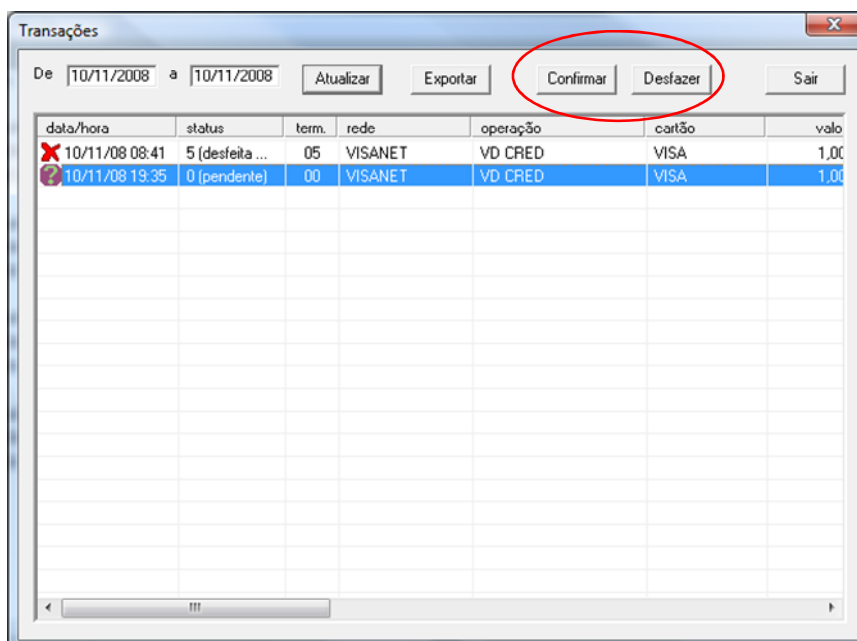
Esta situação pode ser identificada pela mensagem "TERMINAL BLOQUEADO - TRANSACAO PENDENTE". No **Cliente Pay&Go** para Microsoft Windows, esta aparece da seguinte maneira:



A situação também pode ser identificada pelo status da aplicação no **Servidor Pay&Go**:



Para que o terminal virtual volte a operar normalmente, o operador deverá acessar a tela de Consulta de transações no **Servidor Pay&Go** (conforme página 13). Ao selecionar a transação pendente, dois botões adicionais são ativados, o primeiro para confirmar a transação e o segundo para desfazê-la:



É através destes botões que o operador deverá indicar o resultado final da transação, para que o terminal virtual volte a ser ativo.

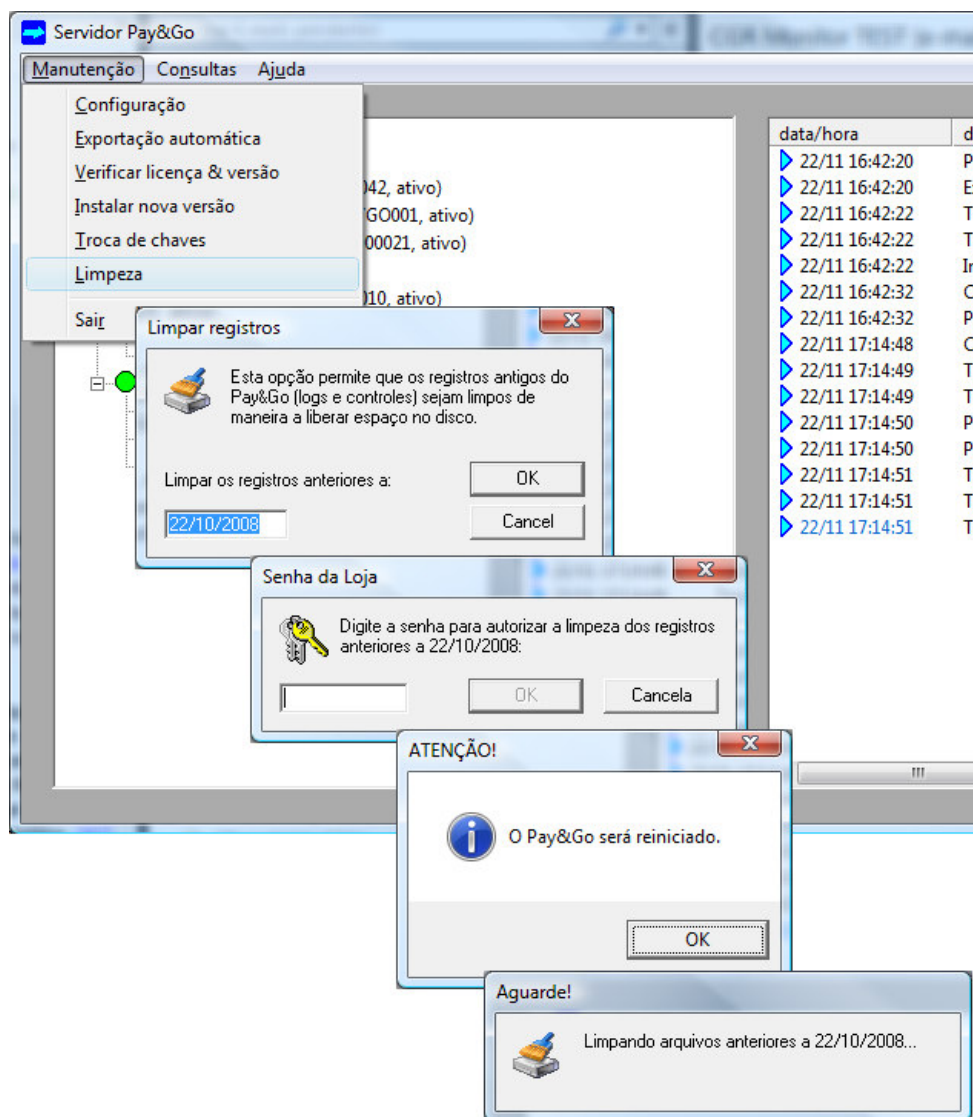
IMPORTANTE: Esta operação não poderá ser desfeita.

Limpeza de registros

O **Servidor Pay&Go** gera diversos arquivos no disco rígido da máquina, para o armazenamento do histórico de transações e logs para depuração do sistema. Estes arquivos tendem a crescer com o tempo, consumindo espaço em disco. É recomendável que, periodicamente, seja feita uma limpeza destes arquivos.

Para isso, deve-se acionar a opção "Limpeza" do menu "Manutenção". Em seguida, o **Servidor Pay&Go**:

- Solicita uma data, de maneira a eliminar todos os registros anteriores a ela;
- Solicita a Senha da Loja (senha padrão: "**1111**");
- É automaticamente reiniciado (após conclusão das eventuais transações em curso);
- Realiza a limpeza (alguns segundos);
- Volta a operar normalmente.



IMPORTANTE: Esta operação deve periodicamente ser realizada, de acordo com o capítulo "Conformidade e Segurança", página 22.

Gerenciamento Remoto

O Pay&Go precisa comunicar-se periodicamente com a Central de Gerenciamento Remoto (CGR) para execução das seguintes tarefas:

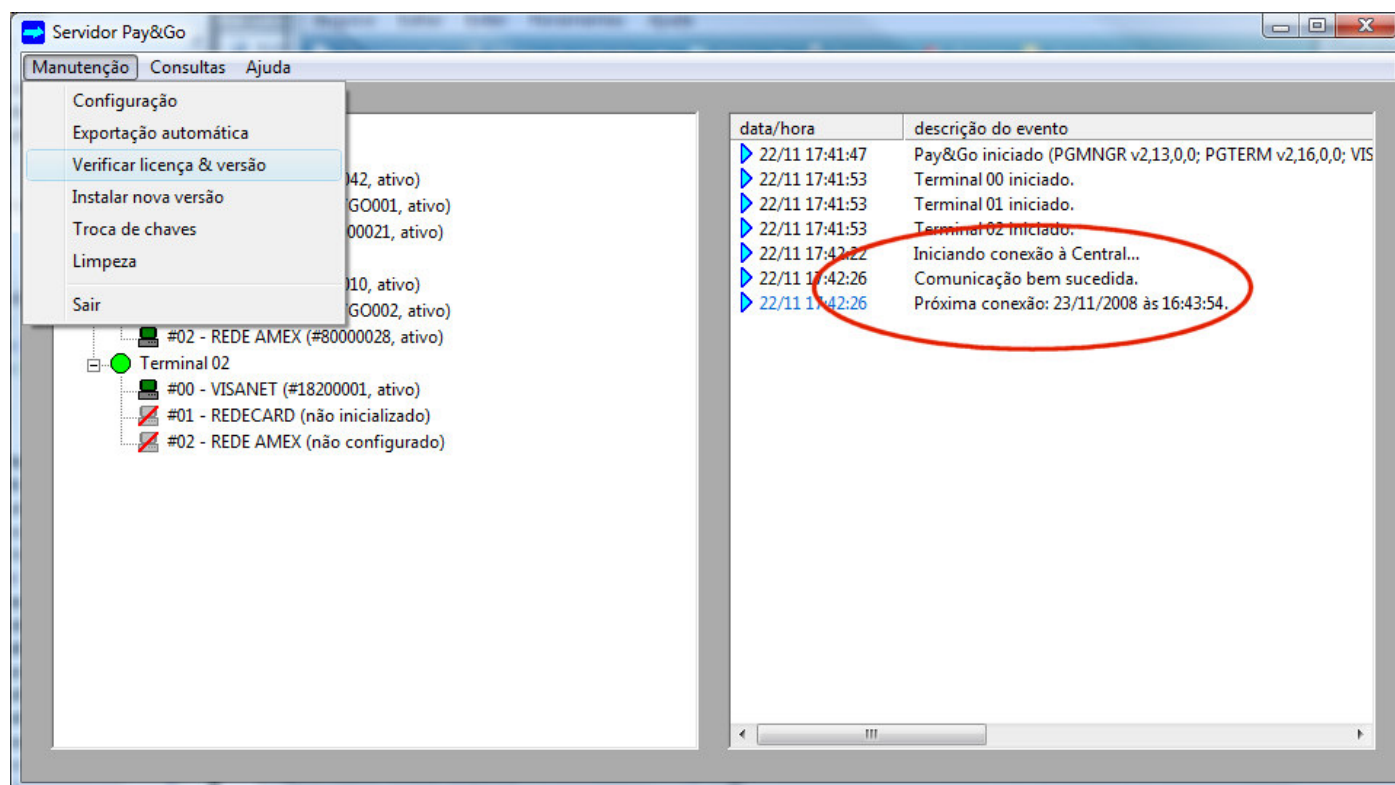
- Renovação da licença de uso do produto;
- Atualização de parâmetros de operação;
- Atualização da versão dos aplicativos que compõem a solução;
- Monitoração do correto funcionamento da solução.

Esta comunicação é sempre iniciada pelo **Servidor Pay&Go** (do estabelecimento para o CGR) através da mesma VPN utilizada para comunicação com as Redes adquirentes e é realizada:

- Manualmente pelo técnico no ato da instalação (uma única vez);

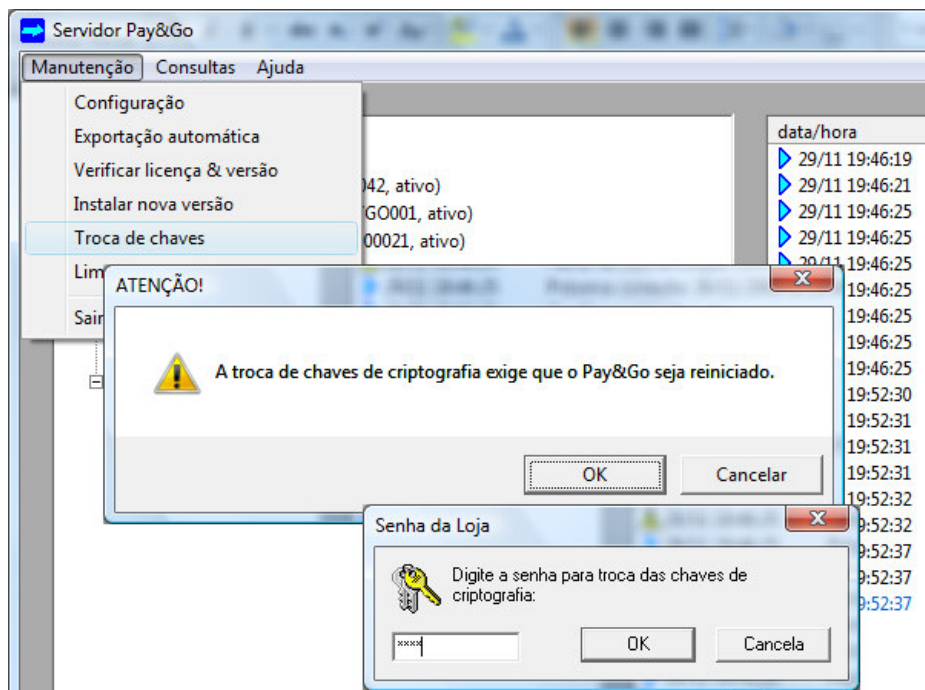
→ Automaticamente, numa frequência configurável no CGR, enquanto o produto permanecer com licença válida.

Caso necessário, esta comunicação pode ser acionada pelo operador através da opção "Verificar licença e versão" do menu "Manutenção":



Troca de chaves

O **Pay&Go Servidor** utiliza internamente várias chaves de criptografia para o armazenamento temporário e seguro de informações sensíveis. Estas chaves são periódica e automaticamente trocadas pelo próprio aplicativo. No entanto, em caso de suspeição de comprometimento da máquina, o operador pode ele mesmo realizar uma troca destas chaves através do menu "Manutenção", item "Troca de chaves":



Após digitação da Senha da Loja (senha padrão: "**1111**"), os terminais virtuais serão desativados (aguardando a conclusão de eventuais transações em curso), a troca de chaves será efetuada e o **Pay&Go Servidor** será automaticamente reiniciado.

Observação: para maiores informações referentes à segurança, consultar o capítulo "Conformidade e Segurança" (página 22).

CONFORMIDADE E SEGURANÇA

O **Pay&Go**, sendo uma solução de pagamento eletrônico, manipula informações sigilosas referentes ao cliente e seu meio de pagamento (cartão). Os aplicativos que compõem a solução **Pay&Go** já fazem uso de recursos avançados para proteger estas informações (retenção mínima, criptografia, etc.). No entanto, para que o estabelecimento esteja em conformidade perante as Redes adquirentes, o ambiente no qual o produto opera também deve respeitar regras básicas de segurança.

O propósito deste capítulo é elencar estas regras, cujo conhecimento e aplicação é indispensável por:

- Funcionários do estabelecimento responsáveis pelo gerenciamento do produto;
- Técnicos de revendedores e integradores envolvidos na instalação do produto.

Uso do PIN-pad

O PIN-pad é um equipamento seguro que atende a especificações rígidas das Redes adquirentes, pois manuseia informações sensíveis referentes ao cartão e ao seu portador. Por isso:

- Somente devem ser utilizados equipamentos devidamente certificados e autorizados pelas Redes adquirentes.
- No ato da instalação do **Pay&Go**, cada equipamento é associado de maneira única a um checkout, sendo proibida a substituição do equipamento por outro ou ainda a troca entre checkouts, ainda que seja dentro do mesmo estabelecimento. Caso haja esta necessidade, o serviço de suporte à solução **Pay&Go** deve ser acionado.
- A troca ou substituição do equipamento PIN-pad por conta própria do estabelecimento pode caracterizar uma tentativa de fraude para as Redes adquirentes, pois o uso desse equipamento é controlado diretamente pelos sistemas de segurança das empresas envolvidas.

Dados históricos

Dados históricos referentes às transações realizadas devem periodicamente ser removidos, conforme detalhado em "Limpeza de registros", página 18.

Coleta de arquivos

Arquivos de uso interno do produto nunca devem ser coletados (copiados, movidos ou enviados para outro equipamento). A única exceção permitida é para resolução esporádica de um problema específico, sempre respeitando as seguintes regras:

- Armazenar os arquivos coletados em um local específico, conhecido e com acesso limitado;
- Coletar somente a quantidade mínima de arquivos necessária à resolução do problema específico;

- Remover todos os arquivos coletados imediatamente após o uso.

Configuração de contas de usuário

Para todos os equipamentos instalados na mesma rede local utilizada para o pagamento eletrônico, as seguintes regras devem ser respeitadas:

- Todas as contas padrão de devem ser desabilitadas, por exemplo:
 - "Administrador" ou "Administrator" para Microsoft Windows;
 - "sa" para Microsoft SQL Server.
- Criar uma conta ("login") específica e individual para cada usuário, não utilizar contas de grupo ou compartilhadas.
- Autenticar cada usuário com pelo menos um dos mecanismos seguintes:
 - Senha (ver restrições abaixo);
 - Autenticação biométrica;
 - Dispositivo de identificação física.
- Em relação às senhas associadas às contas:
 - Não utilizar senhas genéricas;
 - Solicitar a mudança a cada 90 dias, impedindo o uso de uma das 4 senhas anteriormente utilizadas;
 - Exigir uma senha complexa de pelo menos 7 caracteres, contendo ao mesmo tempo caracteres numérica e alfabéticos;
 - Bloquear a conta de usuário após 6 tentativas;
 - Criar uma senha única para cada usuário na ativação da conta e forçar a mudança desta na primeira conexão.
- Bloquear a conta de usuário após 6 tentativas de autenticação sem sucesso, por no mínimo 30 minutos ou até intervenção do administrador.
- Bloquear a sessão após 15 minutos de inatividade, obrigando nova autenticação do usuário.
- Revogar imediatamente conexão de usuários bloqueados/cancelados.
- Remover as contas de usuário inativas a cada 90 dias.

Monitoração

O estabelecimento deve habilitar registros de auditoria para poder reconstruir os seguintes eventos:

- Qualquer acesso por qualquer usuário a um dos equipamentos onde está instalado um dos módulos do sistema **Pay&Go**.
- Todas as ações efetuadas por usuários com privilégios de administrador nestes mesmos equipamentos.
- Qualquer acesso (alteração ou reinicialização) aos registros de auditoria.
- Tentativas de autenticação rejeitadas pelo sistema operacional.

Cada de registro de auditoria deve incluir pelo menos as seguintes informações:

- Identificação do usuário;
- Data e hora;
- Origem do evento (equipamento e módulo de sistema);
- Natureza do evento (motivo do registro);
- Indicação de sucesso ou falha da operação que originou o registro;
- Identificação do objeto/recurso envolvido na operação.

Atualização de sistemas e equipamentos

Todo e qualquer equipamento instalado na mesma rede local utilizada para o pagamento eletrônico deve sempre ser mantido atualizado para corrigir falhas de segurança existentes, seja nos aplicativos, sistemas operacionais ou *firmware*.

Isto significa que:

- O estabelecimento deve manter-se informado em relação às atualizações de segurança disponibilizadas por cada fornecedor (por exemplo através de listas de distribuição).
- Quando possível, os equipamentos devem ser configurados para receber de maneira segura e instalar automaticamente as atualizações de segurança.
- Não devem ser utilizados sistemas ou equipamentos para os quais o fornecedor não disponibiliza mais atualizações de segurança (ou seja, que não são mais suportadas), por exemplo:
 - Versões de Microsoft Windows 9x e anteriores;
 - Versões DOS (Microsoft e outras).

Configuração de equipamentos e rede

Para estabelecimentos que operem com conexão de banda larga:

- Os equipamentos utilizados para o pagamento eletrônico (aqueles onde está instalado um dos módulos do sistema Pay&Go) não devem ser acessíveis pela internet, ou seja um perímetro de firewalls deve impedir toda e qualquer conexão entrante nestes equipamentos a partir da internet.

Para estabelecimentos que operem com conexão GPRS:

- Somente deve ser utilizado o modem fornecido junto com a solução.
- O estabelecimento não deve alterar as configurações do modem. Em caso de necessidade, o suporte à solução **Pay&Go** deve ser acionado.
- Um aplicativo de firewall individual deve ser instalado/configurado no equipamento onde está instalado o **Pay&Go Servidor**, impedindo conexões entrantes pelo modem.

Configuração de redes sem fio

Para estabelecimentos que utilizem redes sem fio, as seguintes regras adicionais devem ser aplicadas:

- Um perímetro de firewalls deve ser instalado e configurado para bloquear ou limitar ao estritamente necessário o tráfego entre as redes sem fio e a rede local utilizada para o pagamento eletrônico.
- Habilitar mecanismos de autenticação e confidencialidade fortes como WPA ou WPA2.
- O padrão WEP não é suficiente para assegurar autenticação e confidencialidade e, caso seja usado, as seguintes regras adicionais se aplicam:
 - Utilizar adicionalmente uma das tecnologias VPN IPsec ou SSL/TLS;
 - Utilizar no mínimo uma chave de criptografia de 104 bits e um vetor de inicialização de 24 bits.
 - Trocar trimestralmente as chaves compartilhadas WEP;
 - Trocar as chaves compartilhadas WEP sempre que houver uma mudança no quadro de funcionários que têm acesso ao roteador;
 - Restringir o acesso sem fio por filtro de endereço MAC.

Acesso remoto

Não é permitido o acesso remoto aos equipamentos utilizados para o pagamento eletrônico. Caso haja uma real necessidade, por exemplo, para resolução de problemas, este pode ser temporariamente ativado em caráter excepcional, sempre em acordo com as seguintes regras:

- As configurações específicas nos firewalls e roteadores para permitir o acesso remoto devem ser habilitadas exclusivamente para o curto período necessário, e desabilitadas imediatamente após o uso.
- Obrigar uma autenticação de dois fatores para o acesso remoto, por exemplo:
 - Usuário/senha e certificado;
 - Usuário/senha e *token*.
- Somente habilitar o acesso remoto por endereços IP ou MAC previamente cadastrados.
- Cifrar todos os dados transmitidos durante a sessão de acesso remoto, através de IPsec, SSL/TLS ou SSH.
- Aplicar também as regras definidas nas seções "Configuração de contas de usuário" (página 23) e "Monitoração" (página 23).

Outros requerimentos

As informações do cartão do cliente (número, data de vencimento, código de segurança, senha, dados contidos na tarja magnética ou no chip, etc.) somente devem ser utilizadas pelo estabelecimento para realização do pagamento eletrônico através da solução **Pay&Go**. Estas informações nunca devem ser retidas/anotadas ou transmitidas.