

Soluções InfinityQS para os Requisitos da FDA CFR 21 Parte 11

- Saiba como manter registros e assinaturas eletrônicas em concordâncias com os Requisitos da FDA CFR 21 Parte 11

O Sistema *InfinityQS* possui uma série de características que o torna uma solução ideal para empresas que são regulamentadas pelos requisitos da FDA (*Food and Drug Administration*). A FDA é a agência americana responsável pela regulamentação de Empresas de Alimentos e Bebidas, Equipamentos Médicos, Medicamentos e Cosméticos que produzem, processam, embalam, ou armazenam produtos que possam vir a ser consumidos nos Estados Unidos.

Em complemento ao sistema de Controle Estatístico de Processo e Qualidade, o *InfinityQS* fornece suporte total aos requisitos da CFR 21 Parte 11 “*Electronic Records, Electronic Signatures*” (norma da agência americana para controle de remédios e alimentos, que regulamenta a segurança de dados e autorizações/autenticações).

A *InfinityQS*® tem permitido à empresas como *Abbott Labs*®, *Novartis*®, *Cordis*®, *Alcon*® e *Baxter*®, a reduzir custos, aumentar eficiência e cumprir com os requisitos de regulamentação. Características como **Gráficos de Genealogia do Lote** e as opções de rastreabilidade têm ajudado os fabricantes de medicamentos a identificar exatamente onde e quando cada componente foi inserido no processo de manufatura.

Abaixo, estão descritas algumas das funcionalidades de segurança fornecidas pelo Sistema *InfinityQS ProFicient*:

- ✓ **Controle de Acesso:** Apenas indivíduos autorizados são capazes de acessar os registros, executar ações controladas ou modificar registros.
- ✓ **Senha Criptografada:** Administradores do sistema não possuem acesso às senhas dos usuários.
- ✓ **Senha de Segurança:** Nenhum outro usuário a não ser o próprio dono do *ID*, poderá acessar sua senha.
- ✓ **Singularidade da Senha:** Cada combinação de *ID* e senha é única.
- ✓ **Idade Máxima da Senha:** Possibilidade de definir que a senha expire automaticamente depois de certo período de tempo.
- ✓ **Forçar a alteração da Senha:** Requerer ao usuário alterar sua senha após o *login* pela primeira vez no sistema.
- ✓ **Tamanho mínimo da Senha:** Possibilidade de exigir um número mínimo de caracteres para a senha.
- ✓ **Bloquear Conta:** Possibilidade de bloquear o usuário após um certo número de tentativas falhas de *login* no sistema. Para desbloquear o *login* do usuário, é necessária a intervenção de um usuário administrador do sistema.

Para um maior esclarecimento, as seções a seguir apresentam a tradução em detalhes dos requisitos da **FDA CFR 21 Parte 11**. Incorporado ao texto destacado em cinza, encontram-se as soluções da *InfinityQS*® e *HarboR Informática Industrial*, descrevendo as funcionalidades embutidas na arquitetura do Sistema responsáveis pelo cumprimento de tais requisitos.

Requisitos da FDA 21 CFR Parte 11

PARTE 11 — Registros Eletrônicos; Assinaturas Eletrônicas (*ELECTRONIC RECORDS; ELECTRONIC SIGNATURES*)

Subparte A—Disposições Gerais

11.1 Scopo.

11.2 Implementação.

11.3 Definições.

Subparte B—Registros Eletrônicos

11.10 Controles para sistemas fechados.

11.30 Controles para sistemas abertos.

11.50 Manifestações de assinaturas.

11.70 Atribuição da assinatura ao registro.

Subparte C—Assinaturas Eletrônicas

11.100 Requisitos Gerais.

11.200 Controle e Componentes da Assinatura Eletrônica.

11.300 Controles para identificação de códigos/senhas.

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

Subparte A—Disposições Gerais

§ 11.1 Scopo

- a. A regulamentação da presente parte estabelece os critérios utilizados pela agência em consideração a registros eletrônicos, assinaturas eletrônicas e assinaturas manuscritas, utilizadas em registros eletrônicos de caráter confiável, seguro, e geralmente o equivalente a registros e assinaturas executadas em papel.
- b. Esta parte aplica-se aos registros em formato eletrônico que são criados, modificados, mantidos, arquivados, recuperados ou transmitidos, sob qualquer requisito relacionado aos regulamentos estabelecidos pela agência. Esta parte também se aplica aos registros eletrônicos apresentados aos organismos regidos pelo *Federal Food, Drug, and Cosmetic Act and the Public Health Service Act*, mesmo que tais registros não sejam especificamente identificados nos regulamentos da agência. No entanto, esta parte não se aplica aos registros de papel que são, ou foram transmitidos por meios eletrônicos.
- c. Quando as assinaturas e registros eletrônicos associados satisfazem os requisitos da presente parte, a agência irá considerar que as assinaturas eletrônicas são equivalentes às assinaturas manuscritas, iniciais, e outras constatações gerais, conforme exigido pela regulamentação da agência, salvo exceções previstas no(s) regulamento(s) efetivo(s) a partir de 20 de agosto de 1997.
- d. Os registros eletrônicos que satisfaçam os requisitos desta parte podem ser utilizados no lugar de registros em papel, em conformidade com o § 11.2, a menos que os registros em papel sejam exigências específicas.
- e. Sistemas de computador (incluindo *hardware* e *software*), controles e assistentes de documentação mantidos em acordo com a presente parte, devem estar prontamente disponíveis e sujeitos a inspeção pela FDA.

§ 11.2 Implementação

- a. **Para os registros que devem ser mantidos, mas não submetidos à agência**, as pessoas podem utilizar os registros eletrônicos em vez de registros em papel, ou assinaturas eletrônicas, em vez de assinaturas tradicionais, no todo ou em parte, desde que os requisitos da presente parte sejam cumpridos.

Os aplicativos da *InfinityQS*® capturam e armazenam registros quantitativos e qualitativos em um banco de dados centralizado. Esses registros são mantidos e controlados em um ambiente seguro, com controle de acesso rigoroso baseado nos requisitos da CFR 21 Parte 11. O acesso ao sistema é gerido através de uma política global de segurança e por meio de privilégios de acesso baseados no usuário. Além disso, o monitoramento e rastreamento histórico de alterações fornece informações para uma auditoria completa e abrangente de qualquer acesso ou alterações nos registros mantidos pelo sistema *InfinityQS*.

- b. Para registros submetidos à agência, as pessoas podem utilizar os registros eletrônicos no lugar de registros em papel ou assinaturas eletrônicas no lugar de assinaturas tradicionais, no todo ou em parte, desde que:
1. Os requisitos desta parte sejam atendidos e
 2. O documento ou partes de um documento a ser submetido, sejam identificados em público, súmula n.º 92S-0251, como possuindo o formato eletrônico aceito pela agência. Esta súmula vai identificar especificamente que tipos de documentos ou partes de documentos são aceitáveis para a apresentação em formato eletrônico, sem registros em papel, e a qual unidade de recebimento (por exemplo, centro específico, escritório, divisão, filial) para que tais submissões possam ser feitas. Documentos enviados às unidades de recebimento que não forem especificados no rol público não serão considerados oficiais se apresentados em formato eletrônico. Os documentos em papel de tais informações serão considerados oficiais e devem acompanhar todos os registros eletrônicos. As pessoas podem consultar a agência de recebimento para obter detalhes sobre como (por exemplo, o método de transmissão de mídia, formatos de arquivo, e protocolos técnicos) prosseguir com a apresentação por via eletrônica.

Os aplicativos da *InfinityQS*® fornecem um conjunto abrangente de ferramentas para configuração de relatórios, que podem ser gerados para satisfazer a maioria das necessidades específicas de clientes e regulamentações. Os relatórios podem incluir um histórico completo de alterações, comentários, eventos e outros dados pertinentes. A *InfinityQS*® pode criar relatórios adicionais com base nas necessidades levantadas pelos clientes.

§ 11.3 Definições

- a. As definições e interpretações dos termos contidos na seção 201 do *act* se aplicam aos termos utilizados nesta parte.
- b. As definições dos termos a seguir também se aplicam a esta parte:
1. **Act** significa *Federal Food, Drug, and Cosmetic Act* (secs. 201–903 (21 U.S.C. 321–393)).
 2. **Agência** refere-se à FDA (*Food and Drug Administration*).
 3. **Biométrica** - método de verificação da identidade de um indivíduo com base na medição das características físicas do indivíduo ou ação repetível onde estas características e/ou ações são mensuráveis e únicas desse indivíduo.
 4. **Sistema fechado** - ambiente no qual o acesso ao sistema é controlado por pessoas que são responsáveis pelo conteúdo dos registros eletrônicos contidos neste sistema.

5. **Assinatura digital** - assinatura eletrônica baseada em métodos criptográficos de autenticação de origem, que é calculado usando um conjunto de regras e parâmetros de tal forma que a identidade do signatário e a integridade dos dados possam ser verificadas.
6. **Registro eletrônico** - qualquer combinação de texto, gráficos, dados, áudio, pictórica, representação ou outras formas de informações em formato digital que seja criado, modificado, mantido, arquivado, recuperado ou distribuído por um sistema de computador.
7. **Assinatura eletrônica** - uma compilação de dados de computador de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser o equivalente juridicamente vinculativo da assinatura manuscrita do mesmo.
8. **Assinatura manuscrita** - *script* ou marco legal de um manuscrito individual executado ou aprovado com a intenção de apresentar uma autenticação permanente na forma escrita. O nome ou marca legal, quando convencionalmente aplicado ao papel, também pode ser aplicado a outros dispositivos que captam o nome ou marca.
9. **Sistema aberto** - ambiente no qual o acesso ao sistema não é controlado por pessoal designado.

Subparte B—Registros Eletrônicos

§ 11.10 Controle para sistemas fechados

Pessoas que utilizam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles destinados a garantir a autenticidade, integridade e, quando necessário, a confidencialidade dos registros eletrônicos, e garantir que o usuário que assina não pode prontamente repudiar os registros assinados como não genuíno. Tais procedimentos e controles devem incluir o seguinte:

A *InfinityQS*® recomenda que os aplicativos *InfinityQS ProFicient* sejam implementados em um sistema fechado para minimizar a necessidade de controles adicionais para assegurar a integridade das informações gerenciadas pelo sistema.

- a. Validação de sistemas para garantir a precisão, confiabilidade, desempenho consistente, bem como a capacidade de discernir registros inválidos ou alterados.

A *InfinityQS*® realiza e mantém uma validação estatística completa das aplicações do *InfinityQS SPC*. Também são fornecidos serviços de consultoria para auxiliar nas documentações e procedimentos de validação.

Quanto aos registros, tabelas auditáveis são usadas para controlar todas as alterações de registro no banco de dados. A utilização de *time stamp* de criação e edição permite que os registros alterados sejam facilmente detectados.

➤ **Início - Configurações Necessárias no Sistema**

Com as opções de rastreabilidade do Sistema, todas as modificações de registros são registradas nas tabelas de rastreabilidade criadas para cada tabela ativa do *ProFicient*. Estes registros não são exibidos em tabelas separadas, mas sim como linhas adicionais destacadas em amarelo e nos campos de auditoria e rastreabilidade.

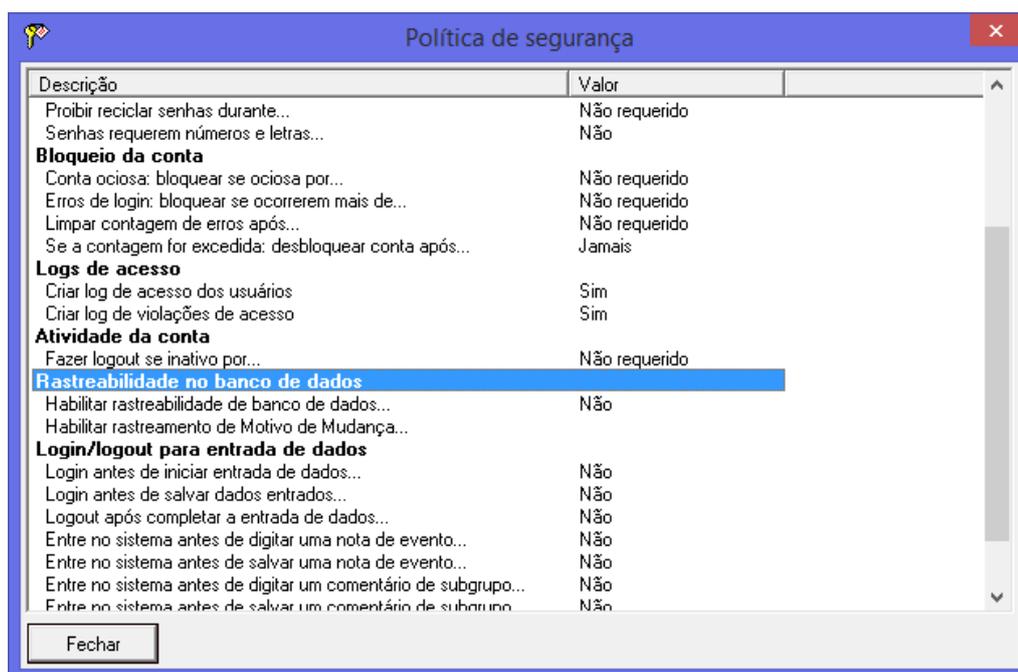
Rastreabilidade de Modificação de Registro. Antes de alterar o dado, o *ProFicient* copia o registro original para a tabela de rastreabilidade com todos os campos de rastreabilidade, assegurando um completo histórico de alterações do banco de dados.

Rastreabilidade de Exclusão de Registro. Enquanto o *ProFicient* não exclui de fato nenhum registro no banco de dados, ele permite que certos usuários (por exemplo, administradores) possam alterar o status dos registros para *Excluídos*, indicando que o registro está indisponível. Como descrito no item acima, o *ProFicient* copia o registro original para a tabela de rastreabilidade antes de atualizar o *status*, e registra o usuário e a hora em que o *status* foi excluído.

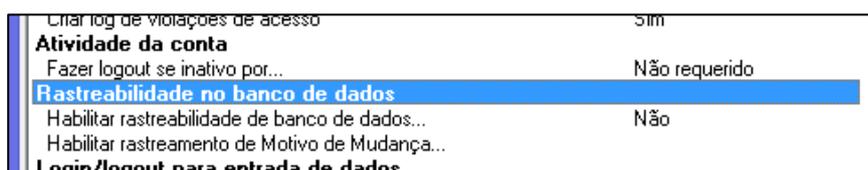
Campos de Auditoria/Rastreabilidade. O *ProFicient* exibe a partir do *Database Manager*, os seguintes campos para cada registro:

- **Data de Criação.** Registra a data e hora de criação.
- **Última Edição.** Registra a data e hora da modificação.
- **Usuário.** Usuário conectado no *ProFicient* quando o registro foi criado ou modificado.
- **Desativar.** Status atual do registro.
- **Motivo.** Razão da modificação inserida pelo usuário.

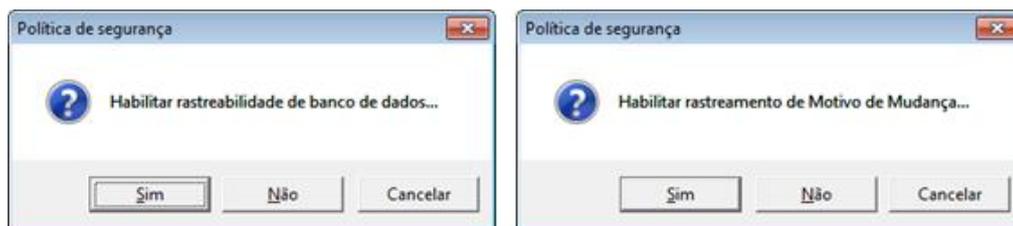
1. Acesse o *Database Manager* e faça o *login* no banco de dados desejado.
2. Na barra de menu, clique **Preferências | Política de segurança**, a janela **Política de segurança** abrirá.



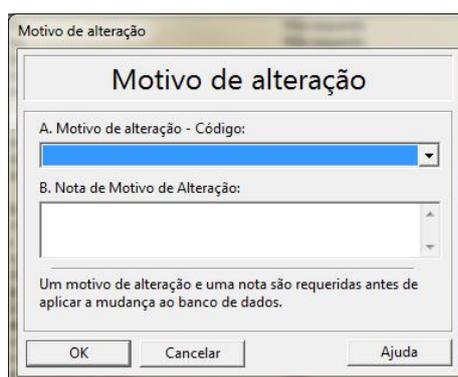
3. Localize a seção **Rastreabilidade no banco de dados**.



4. Na seção **Rastreabilidade no banco de dados**, dê um duplo clique nas opções **Habilitar rastreabilidade de banco de dados** e **Habilitar rastreamento de Motivo de Mudança** e clique em **SIM** para habilitar as opções.

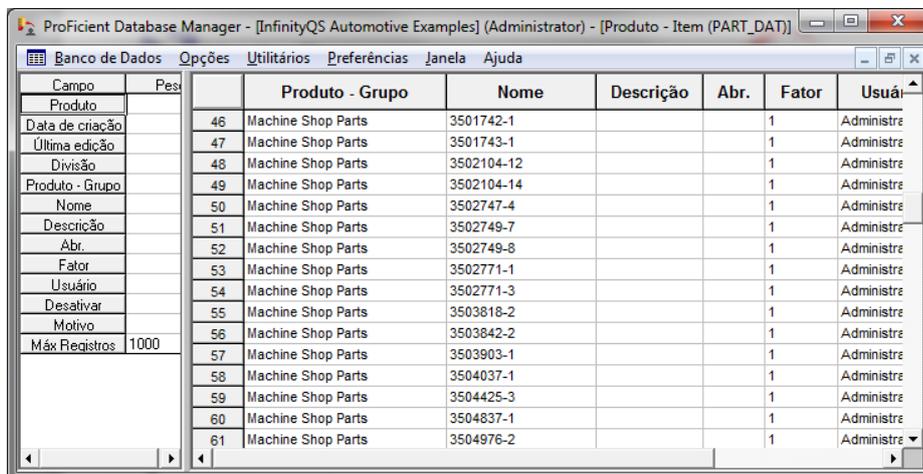


Com a opção de rastrear os motivos ativada, é solicitado ao usuário inserir uma explicação/motivo para qualquer modificação que seja realizada no banco de dados (nomes de produtos, processos, testes, limites de controle, limites de especificação, valores de teste, funcionários, etc.), gerando relatórios com os resumos das modificações.



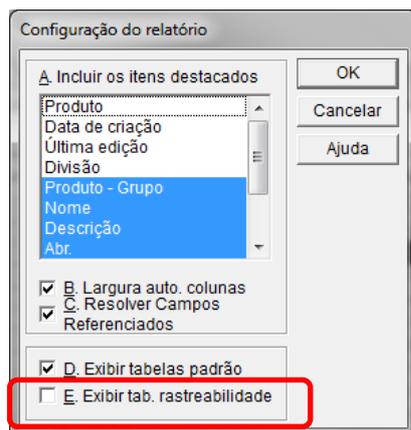
Configurando Campos de Rastreabilidade nas Tabelas

1. A partir do *Database Manager*, abra a tabela desejada.



Campo	Pesq	Produto - Grupo	Nome	Descrição	Abr.	Fator	Usuário
Produto							
Data de criação		46	Machine Shop Parts	3501742-1		1	Administr
Última edição		47	Machine Shop Parts	3501743-1		1	Administr
Divisão		48	Machine Shop Parts	3502104-12		1	Administr
Produto - Grupo		49	Machine Shop Parts	3502104-14		1	Administr
Nome		50	Machine Shop Parts	3502747-4		1	Administr
Descrição		51	Machine Shop Parts	3502749-7		1	Administr
Abr.		52	Machine Shop Parts	3502749-8		1	Administr
Fator		53	Machine Shop Parts	3502771-1		1	Administr
Usuário		54	Machine Shop Parts	3502771-3		1	Administr
Desativar		55	Machine Shop Parts	3503818-2		1	Administr
Motivo		56	Machine Shop Parts	3503842-2		1	Administr
Máx Registros	1000	57	Machine Shop Parts	3503903-1		1	Administr
		58	Machine Shop Parts	3504037-1		1	Administr
		59	Machine Shop Parts	3504425-3		1	Administr
		60	Machine Shop Parts	3504837-1		1	Administr
		61	Machine Shop Parts	3504976-2		1	Administr

2. Na tabela desejada, clique com o botão direito em qualquer registro, e então clique na opção **Configuração do Relatório**. A tela **Configuração do relatório** será exibida.



3. Na tela **Configuração do relatório**, marque a opção **Exibir tab. Rastreabilidade**. Esta opção ativa também a coluna de Auditoria na tabela.

	Divisão	Produto - Grupo	Nome	D
1	<undefined>	Wheel Spindles	%MAYMWE	
2	<undefined>	Wheel Spindles	%MAYMWEY	
3	<undefined>	Wheel Spindles	%MAYMWEYY	
4	<undefined>	Wheel Spindles	%MAYMWEYYY	
5	<undefined>	Wheel Spindles	%MAYMWEYYY%	
6	Consumer Products	Gage Blocks	1.00 Block	
7	<undefined>	Produtos Maxforja	1.633.703.000	
8	Division	Innovative Charting Parts List	-101 Part	
9	Consumer Products	Engine Components	12768-10E	Sta
10	Consumer Products	Gage Blocks	2.00 Block	

➤ **Fim**

- b. Capacidade de gerar cópias precisas e completas de registros em formato eletrônico e formato legível, adequados para inspeção, revisão e cópia pela agência. As pessoas devem contatar a agência, se houver qualquer dúvida quanto à capacidade do organismo para realizar essa fiscalização das cópias dos registros eletrônicos.

Os pacotes do *software InfinityQS ProFicient* incluem um vasto conjunto de relatórios que podem ser gerados em forma de cópia eletrônica ou forma impressa. Os relatórios incluem o histórico completo de alterações e razões de alterações, bem como funções necessárias para regenerar o relatório em uma data posterior.

➤ **Início - Configurações Necessárias no Sistema**

Para criar relatórios ou gráficos no *InfinityQS SPC MI* um projeto deve primeiramente ser criado.

1. Abra o *SPC MI*, faça o *login* no banco de dados desejado e crie ou abra um projeto já existente.
2. Na barra de menu do projeto, clique **Gráfico | Novo**, a janela **Nome** abrirá.
3. Faça as configurações do gráfico passando pelas etapas de criação a partir dos botões **AVANÇAR** ou **VOLTAR**.
4. Na janela **Seleção de Dados do Subgrupo**, clique em terminar para criar o gráfico.

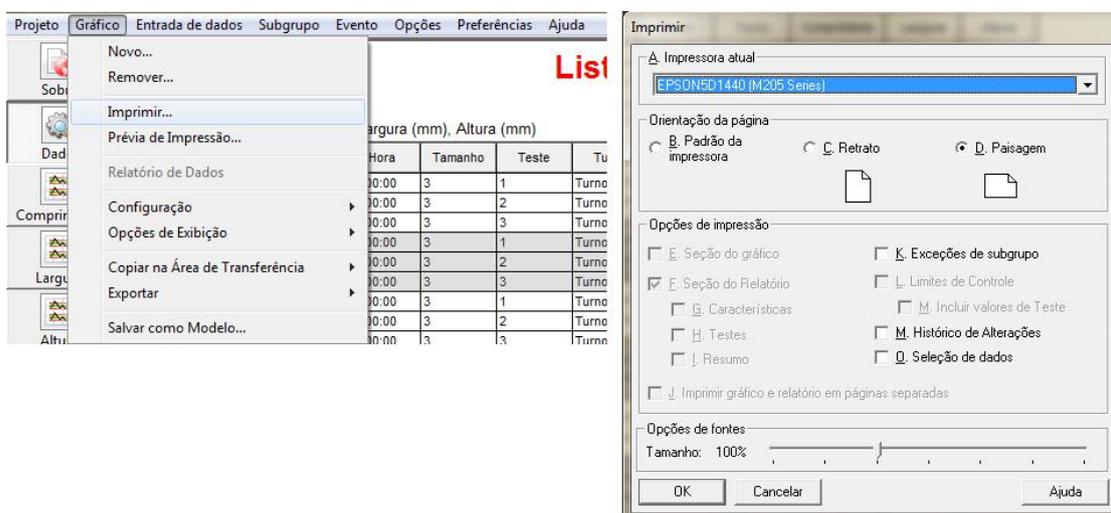
Após criar o gráfico, ele fica disponível tanto para impressão quanto para cópias eletrônicas.

Lista de Dados Detalhados da Produção

Produto: Bolo c/ Cobertura
Processo: Bolos - Linha 2
Teste: Comprimento (mm), Largura (mm), Altura (mm)

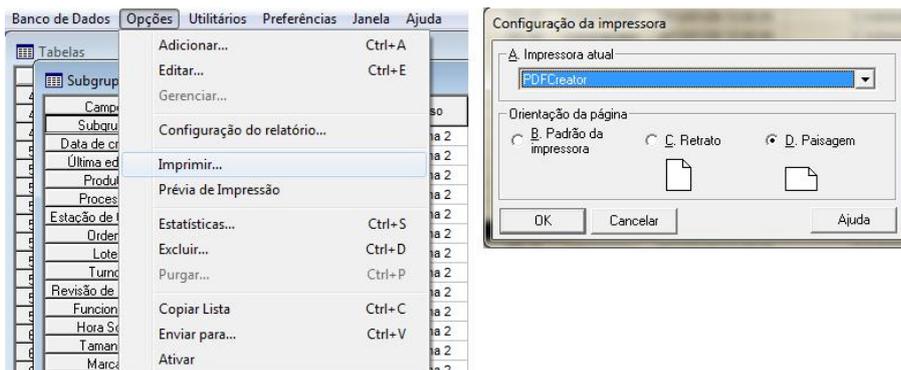
Lote	Funcionário	Data	Hora	Tamanho	Teste	Turno	Comprimento	Largura	Altura
BP-55	Administrato	31/01/2012	07:00:00	3	1	Turno 3			15,0000
BP-55	Administrato	31/01/2012	07:00:00	3	2	Turno 3			14,9950
BP-55	Administrato	31/01/2012	07:00:00	3	3	Turno 3			15,0000
BP-55	Administrato	31/01/2012	08:00:00	3	1	Turno 2	82,5150		
BP-55	Administrato	31/01/2012	08:00:00	3	2	Turno 2	82,5150		
BP-55	Administrato	31/01/2012	08:00:00	3	3	Turno 2	82,5900		
BP-55	Administrato	31/01/2012	05:00:00	3	1	Turno 2			14,9950
BP-55	Administrato	31/01/2012	05:00:00	3	2	Turno 2			14,9950
BP-55	Administrato	31/01/2012	05:00:00	3	3	Turno 2			15,0000
BP-56	Administrato	31/01/2012	04:00:00	3	1	Turno 2			15,0150
BP-56	Administrato	31/01/2012	04:00:00	3	2	Turno 2			15,0150
BP-56	Administrato	31/01/2012	04:00:00	3	3	Turno 2			15,0050
BP-56	Administrato	31/01/2012	03:00:00	3	1	Turno 2	82,5750		
BP-56	Administrato	31/01/2012	03:00:00	3	2	Turno 2	82,5750		
BP-56	Administrato	31/01/2012	03:00:00	3	3	Turno 2	82,5750		
BP-56	Administrato	31/01/2012	02:00:00	3	1	Turno 2			15,0150
BP-56	Administrato	31/01/2012	02:00:00	3	2	Turno 2			15,0050
BP-56	Administrato	31/01/2012	02:00:00	3	3	Turno 2			15,0050

- Para imprimir, clique em **Gráfico | Imprimir**. A janela **Imprimir** abrirá. Faça as configurações desejadas para o arquivo de impressão e clique em **OK**.



- Para imprimir uma tabela do banco de dados, abra a tabela desejada e em seguida clique em **Opções | Imprimir**. A janela **Configuração da Impressora** abrirá. Faça as configurações desejadas para o arquivo de impressão e clique em **OK**.

	Produto	Processo	Estação de trabalho	Lote	Funcionário	Hora Sgrp	Tamanho	Usuário	Desativar	Motivo	Transaction Time
1	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-15	Administrato	2012/01/29 05:00:00	3	Administrato			
2	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/31 06:00:00	3	Administrato			
3	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/31 05:00:00	3	Administrato			
4	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-56	Administrato	2012/01/31 04:00:00	3	Administrato			
5	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-56	Administrato	2012/01/31 03:00:00	3	Administrato			
6	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-56	Administrato	2012/01/31 02:00:00	3	Administrato			
7	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/31 01:00:00	3	Administrato			
8	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/31 00:00:00	3	Administrato			
9	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/30 23:00:00	3	Administrato			
10	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-49	Administrato	2012/01/29 13:00:00	3	Administrato			
11	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-49	Administrato	2012/01/29 12:00:00	3	Administrato			
12	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-49	Administrato	2012/01/29 11:00:00	3	Administrato			
13	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-32	Administrato	2012/01/29 10:00:00	3	Administrato			
14	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-32	Administrato	2012/01/29 09:00:00	3	Administrato			
15	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-32	Administrato	2012/01/29 08:00:00	3	Administrato			
16	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-15	Administrato	2012/01/29 07:00:00	3	Administrato			
17	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-15	Administrato	2012/01/29 06:00:00	3	Administrato			
18	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrato	2012/01/31 07:00:00	3	Administrato			
19	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-15	Administrato	2012/01/29 04:00:00	3	Administrato			



➤ Fim

- c. Proteção dos registros para possibilitar recuperação de maneira precisa durante o período de retenção de registros.

Todos os registros eletrônicos, bem como alterações e justificativas para alterações de registros, são mantidos em um banco de dados centralizado e seguro. O acesso aos dados está limitado a indivíduos ou grupos específicos. Modificação e/ou exclusão de registros é restrito, de maneira a garantir a integridade durante o período de retenção de registros.

➤ Início - Configurações Necessárias no Sistema

O acesso ao banco de dados a partir do *Database Manager* é realizado através de uma senha e *login* individual com permissões específicas para cada usuário.

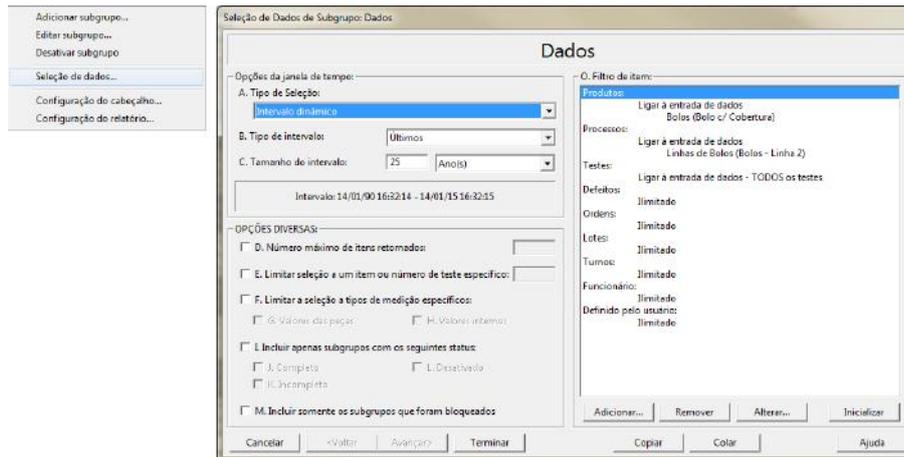


Os subgrupos alterados terão a sua rastreabilidade registrada no banco de dados, na tabela *Subgrupo – Informação (SGRP_INF)*. Os registros em amarelo são aqueles que sofreram a modificação. Na coluna **Motivo** fica registrado o motivo da alteração, quando atribuído. Na coluna **Desativar** fica registrado os subgrupos que foram excluídos com a descrição **Excluir**. Nesta tabela ainda se pode rastrear **Usuário**, **Data de criação**, **Última edição** e outras informações referentes ao subgrupo coletado.

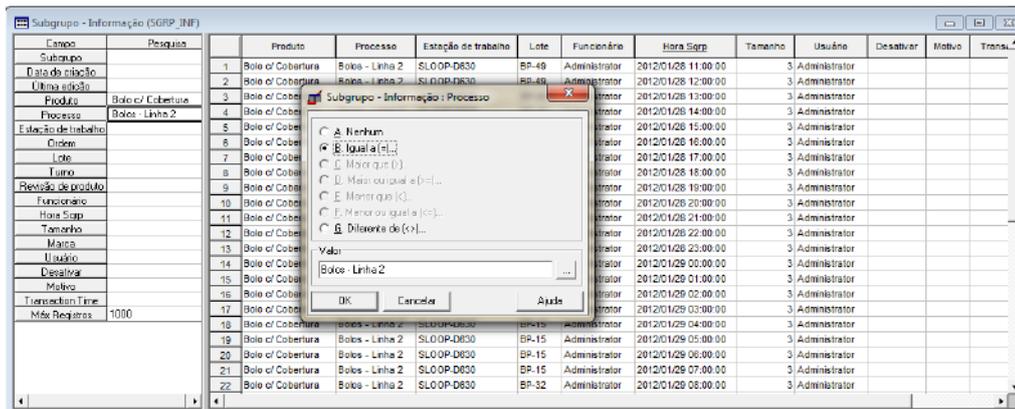
Subgrupo	Data de criação	Última edição	Produto	Processo	Estação de trabalho	Lote	Funcionário	Hora Sgrp	Usuário	Desativar	Motivo	Transaction Time
1418751704	2014/12/16 15:41:44	2014/12/16 15:42:41	Bolo c/ Recheio	Bolos - Linha 2	FREDDIE	YP-49	Administrador	2014/12/16 15:41:24	Administrador		Subgrupo Desativado	2014/12/16 15:42:41
1418751704	2014/12/16 15:41:44	2014/12/16 15:41:44	Bolo c/ Recheio	Bolos - Linha 2	FREDDIE	YP-49	Administrador	2014/12/16 15:41:24	Administrador			2014/12/16 15:41:44
1418750813	2014/12/16 15:26:53	2014/12/16 15:27:39	Bolo c/ Cobertura	Bolos - Linha 2	FREDDIE	BP-60	Administrador	2014/12/16 15:26:21	Administrador		Erro de digitação	2014/12/16 15:27:39
1418750813	2014/12/16 15:26:53	2014/12/16 15:26:53	Bolo c/ Cobertura	Bolos - Linha 2	FREDDIE	BP-60	Operador	2014/12/16 15:26:21	Operador			2014/12/16 15:26:53
1335362238	2012/04/25 10:56:09	2014/12/16 15:23:32	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrador	2012/01/31 07:00:00	Administrador		Erro de digitação	2014/12/16 15:23:32
1335362238	2012/04/25 10:56:09	2014/12/16 16:00:28	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrador	2012/01/31 07:00:00	Administrador	Excluir	Excluir Subgrupo	2014/12/16 15:23:32

Para consultar dados antigos é possível usar diferentes tipos de filtros que facilitam na busca, por exemplo: processos, produto, teste, faixa de datas, etc.

1. Para consultar registros em gráficos e relatórios no *InfinityQS SPC MI*, clique no projeto desejado, clique com o botão direito e selecione a opção **Seleção de Dados**. A janela **Seleção de Dados de Subgrupo: Dados** abrirá.



2. Na janela **Seleção de Dados de Subgrupo: Dados** configure os filtros desejados para a consulta dos dados.
3. Para consultar registros a partir do *Database Manager*, abra a tabela desejada e configure os filtros no canto esquerdo da janela.



Campo	Pesquisa	Produto	Processo	Estação de trabalho	Lote	Funcionário	Hora Sarp	Tamanho	Usuário	Desativar	Motivo	Trans.
Subgrupo		1 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 11:00:00	3	Administrador			
Estado medição		2 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 12:00:00	3	Administrador			
Última ação		3 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 13:00:00	3	Administrador			
Produto	Bolo cf Cobertura	4 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 14:00:00	3	Administrador			
Processo	Bolos - Linha 2	5 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 15:00:00	3	Administrador			
Estação de trabalho		6 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 16:00:00	3	Administrador			
Ordem		7 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 17:00:00	3	Administrador			
Lote		8 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 18:00:00	3	Administrador			
Turno		9 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 19:00:00	3	Administrador			
Revisão de produto		10 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 20:00:00	3	Administrador			
Funcionário		11 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 21:00:00	3	Administrador			
Hora Sarp		12 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 22:00:00	3	Administrador			
Tamanho		13 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/28 23:00:00	3	Administrador			
Usuário		14 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/29 00:00:00	3	Administrador			
Desativar		15 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/29 01:00:00	3	Administrador			
Motivo		16 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/29 02:00:00	3	Administrador			
Transaction Time		17 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/29 03:00:00	3	Administrador			
Máx Registros	1000	18 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-49	Administrador	2012/01/29 04:00:00	3	Administrador			
		19 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-15	Administrador	2012/01/29 05:00:00	3	Administrador			
		20 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-15	Administrador	2012/01/29 06:00:00	3	Administrador			
		21 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-15	Administrador	2012/01/29 07:00:00	3	Administrador			
		22 Bolo cf Cobertura	Bolos - Linha 2	SLOOP-D830	BP-32	Administrador	2012/01/29 08:00:00	3	Administrador			

➤ **Fim**

- d. Acesso ao sistema limitado às pessoas autorizadas.

O acesso aos registros é controlado por meio da utilização de um único par de *login* e senha criptografada de 128 bits. Vários níveis de segurança e controle de acessos limitados para os registros são baseados nas funções e responsabilidades dos usuários.

➤ **Início - Configurações Necessárias no Sistema**

O acesso aos dados é realizado através de uma senha e *login* individual com permissões específicas para cada usuário.

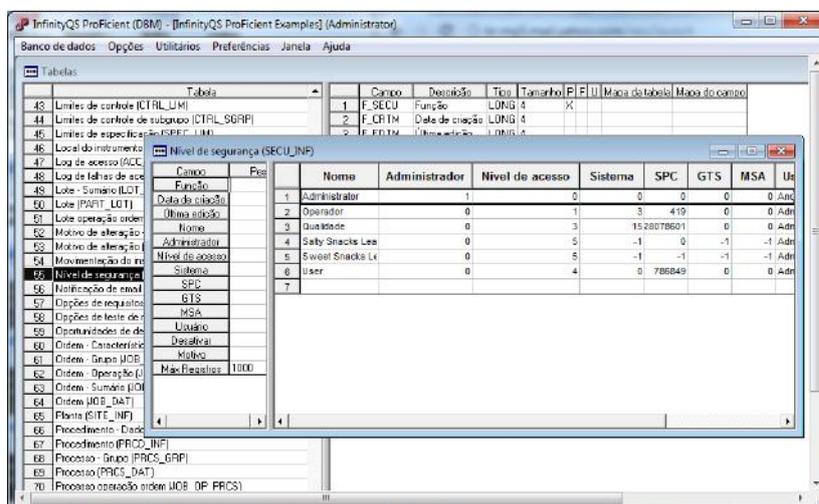


O *InfinityQS* permite que diferentes níveis de segurança sejam criados apenas por usuários administradores. O objetivo da criação destes níveis de segurança é poder atribuir diferentes permissões a diferentes usuários do sistema.

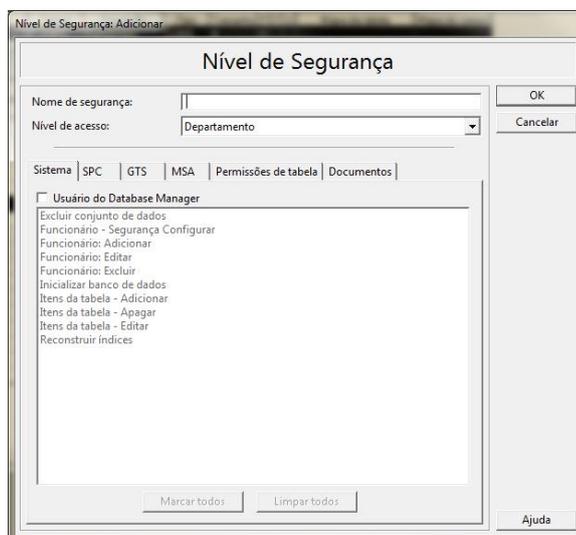
Para criar níveis de segurança é necessário acessar o *Database Manager*. Ao abri-lo, selecione a fonte de dados correspondente ao banco de dados do *InfinityQS*, no qual deseja-se criar o novo nível de segurança, e digite o *login* e a senha.

No *Database Manager*, localize a tabela *Nível de Segurança (SECU_INF)*.

Execute duplo clique sobre a linha referente à tabela *Nível de Segurança*. A janela **Nível de segurança (SECU_INF)** será exibida.



Crie um novo nível de segurança através da janela **Nível de segurança: Adicionar**.



Na janela **Nível de segurança: Adicionar**, nomeie o nível de segurança a ser criado e ative as permissões desejadas.

1. No campo **Nome de segurança** insira um nome ao nível de segurança. Ex: Administrador, Gerente, Operador, etc.
2. No campo **Nível de acesso** atribua o nível de acesso (*Administrador, Banco de Dados, Empresa, Divisão, Planta ou Departamento*) para o nível de segurança.
3. Nas abas **Sistema, SPC, GTS, MSA, Permissões de tabela** e **Documentos** configure as permissões de cada nível. Para ativar um item, basta executar duplo clique sobre a opção desejada.

Após realizar as ativações necessárias, clique em **OK** e o nível de segurança estará criado. Agora, este nível já estará disponível para ser atribuído a um usuário (através da tabela *Funcionário – Informação (EMPL_INF)*).

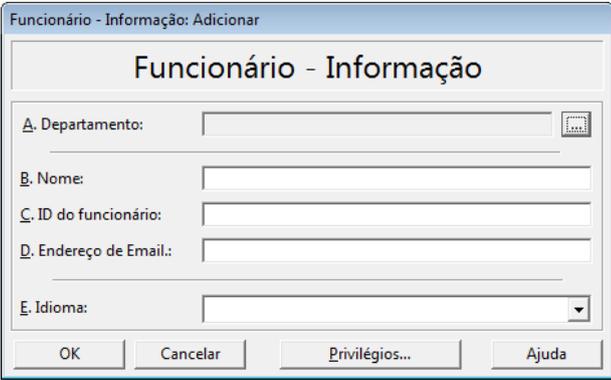
O *InfinityQS* permite o cadastro ilimitado de novos usuários. Ao cadastrar um novo usuário, é atribuído um nível de segurança a ele. Desta forma, é possível controlar todas as permissões deste usuário dentro do sistema.

Para cadastrar novos usuários, acesse a tabela *Funcionário - Informação (EMPL_INF)*. Ao abrir a tabela de Funcionário, é possível verificar todos os usuários cadastrados no banco de dados.



Evento	Evento	Funcionário	Departamento	Nome	Empr. ID	Email	Status	Fator	Usuário	Desativar	Motivo
30	Eventos (EVNT_INF)										
31	Função - Extra (SECU_XTR)										
32	Funcionário - Extra (EMPL_XTR)										
33	Funcionário - Segurança (EMPL_SEC)										
34	Funcionário (EMPL_INF)		1	Departamento	José	José	jose@empresa.com.br	0	0		
35	Idioma - Dados (LNG_DAT)		2								
36	Idioma (LNG_TYPI)										

Abra a janela para cadastro de novos usuários e preencha as informações.



Funcionário - Informação: Adicionar

Funcionário - Informação

A. Departamento:

B. Nome:

C. ID do funcionário:

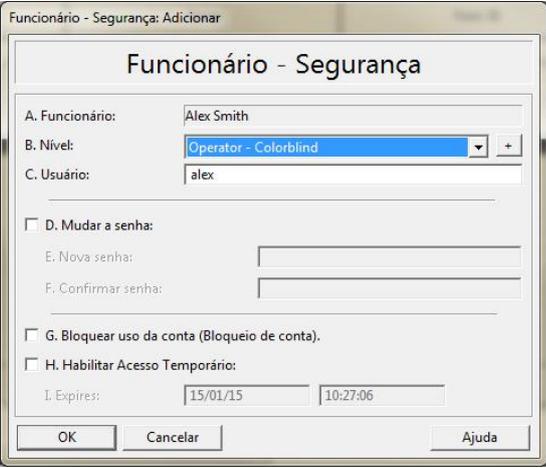
D. Endereço de Email:

E. Idioma:

OK Cancelar Privilegios... Ajuda

1. No campo **Departamento** atribua o departamento a que o funcionário pertence.
2. No campo **Nome** adicione o nome do funcionário.
3. No campo **Endereço de E-mail** adicione o endereço de e-mail do funcionário.
4. No campo **Idioma** selecione o idioma que o funcionário utilizará para acessar o *InfinityQS* (Obs.: em um mesmo banco de dados, é possível que diversos funcionários utilizem idiomas diferentes).

Após preencher os campos, clique em **PRIVILÉGIOS** e preencha o restante das informações.



Funcionário - Segurança: Adicionar

Funcionário - Segurança

A. Funcionário: Alex Smith

B. Nível: Operator - Colorblind

C. Usuário: alex

D. Mudar a senha:

E. Nova senha:

F. Confirmar senha:

G. Bloquear uso da conta (Bloqueio de conta).

H. Habilitar Acesso Temporário:

I. Expires: 15/01/15 10:27:06

OK Cancelar Ajuda

1. O campo **Funcionário** já aparecerá preenchido.

2. No campo **Nível** atribua uma função para o funcionário dependendo dos níveis de segurança cadastrados.
3. No campo **Login** atribua o *login* do usuário.
4. No campo **Mudar a senha** atribua uma senha para *login* do usuário ou troque uma senha já existente.
5. A opção **Bloquear uso da conta** permite bloquear o uso da conta. Para desbloquear o usuário esta opção deve ser desmarcada.
6. A opção **Habilitar Acesso Temporário** permite definir o prazo (data e hora) para que o usuário expire.

➤ **Fim**

- e. Uso de redes seguras e rastreáveis para salvar os dados e as ações de modificar ou excluir os registros eletrônicos. Registros modificados não devem obscurecer as informações registradas anteriormente. Esta documentação de alterações deve ser mantida da mesma maneira que os registros eletrônicos, e devem estar disponíveis para revisão e cópia pela agência.

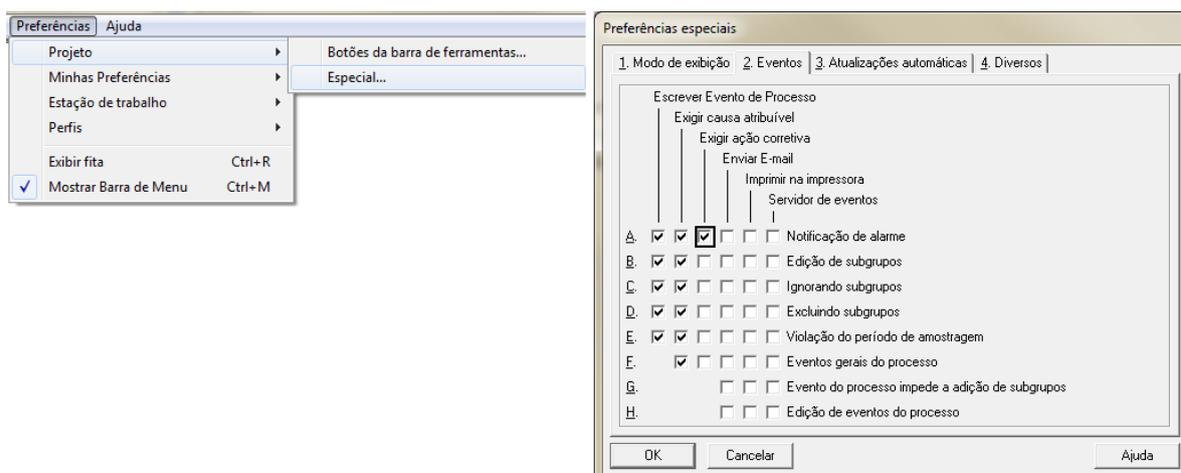
Todos os registros eletrônicos contém um mínimo de dois carimbos de tempo (*time stamps*): hora de criação e hora de edição. Além disso, todos os registros eletrônicos contém informações de identificação do usuário que criou ou modificou o registro. Antes de qualquer alteração em um registro eletrônico estar comprometida com o banco de dados, o registro (inalterado) é copiado para o quadro histórico de mudanças e uma razão para a alteração do registro é criada. Todos os registros de alterações são mantidos durante a vida útil do sistema e podem ser arquivados para fins de manutenção.

➤ **Início - Configurações Necessárias no Sistema**

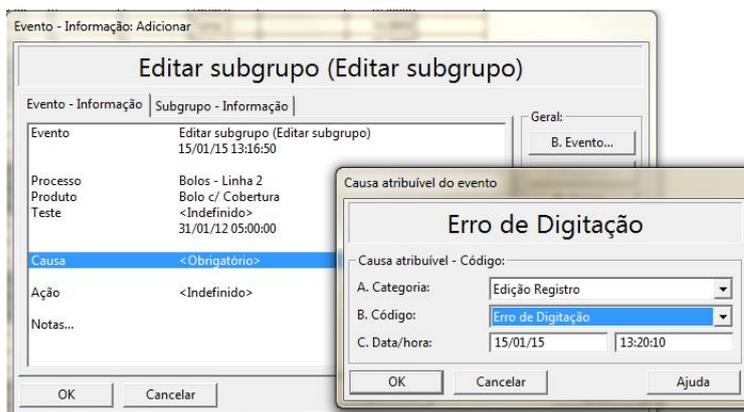
O *InfinityQS* permite opções de configurações para diferentes tipos de alterações que possam ser realizadas nos registros.

Para habilitar estas configurações é preciso acessar o *InfinityQS SPC MI*.

1. Abra o *SPC MI* e faça o *login* no banco de dados desejado e crie ou abra um projeto já existente.
2. Na barra de menu, clique **Preferências | Projeto | Especial**, a janela **Preferências especiais** abrirá.

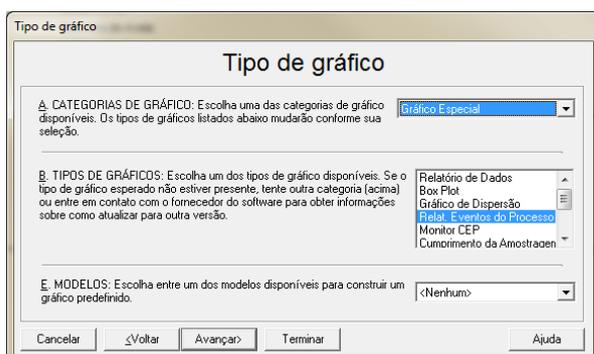


3. Localize a aba **Eventos** e habilite as opções de eventos que desejar. Clique no botão **OK** para salvar as alterações.
Por exemplo, nesta configuração, para cada edição de subgrupo será criado um evento e uma Causa Atribuível deverá ser registrada.



Para visualizar os dados em forma de relatório é preciso criar um Relatório de Eventos do Processo.

1. Na barra de menu, clique **Gráfico | Novo**, a janela **Nome** abrirá.
2. Faça as configurações do gráfico passando pelas etapas de criação a partir dos botões **AVANÇAR** ou **VOLTAR**.
3. Na janela **Tipo de Gráfico**:
 - No campo **Categoria de Gráfico** selecione a opção **Gráfico Especial**.
 - No campo **Tipos de Gráficos** selecione a opção **Relat. Eventos do Processo**.
 - No campo **Modelo** selecione o modelo desejado, se existir.
 - Clique no botão **TERMINAR** e o gráfico será criado.



15/01/2015 13:16:50	Editar subgrupo:	Editar subgrupo (Administrator)
31/01/2012 05:00:00	Processo:	Bolos - Linha 2
	Produto:	Bolo c/ Cobertura
	Lote:	BP-55
	Funcionário:	Administrator
	Turno:	Turno 2
15/01/2015 13:20:10	Causa:	Erro de Digitação (Administrator)
31/01/2012 05:00:00	Tempo transcorrido:	00:03:20
	1:	14,995
	2:	14,995
	3:	15,004

Os registros desabilitados irão aparecer no Relatório de Dados do projeto, na coluna **Status** com a descrição **Ignorado**.

SID	Status	Lote	Funcionário	Data	Hora	Tamanho	Teste	Turno	Comprimento	Largura	Altura
141875704	Ignorado	YP-49	Administrator	16/12/2014	15:41:24	3	1	Turno 1	62,5000	17,5500	15,0000
141875704	Ignorado	YP-49	Administrator	16/12/2014	15:41:24	3	2	Turno 1	62,5000	17,5000	15,0000
141875704	Ignorado	YP-49	Administrator	16/12/2014	15:41:24	3	3	Turno 1	62,3000	17,5000	15,0000
141875813	Ignorado	BP-60	Administrator	16/12/2014	15:26:21	3	1	Turno 1	82,5000	15,0001	15,0060
141875813	Ignorado	BP-60	Administrator	16/12/2014	15:26:21	3	2	Turno 1	82,5000	15,0040	15,0050
141875813	Ignorado	BP-60	Administrator	16/12/2014	15:26:21	3	3	Turno 1	82,4500	15,0005	15,0040

Os subgrupos alterados também terão a sua rastreabilidade registrada no banco de dados, na tabela *Subgrupo – Informação (SGRP_INF)*. Os registros em amarelo são aqueles que sofreram a modificação. Na coluna **Motivo** fica registrado o motivo da alteração. Na coluna **Desativar** fica registrado os subgrupos que foram excluídos com a descrição **Excluir**. Nesta tabela ainda se pode rastrear **Usuário**, **Data de criação**, **Última edição** e outras informações referentes ao subgrupo coletado.

Subgrupo	Data de criação	Última edição	Produto	Processo	Estação de trabalho	Lote	Funcionário	Hora Sgrp	Usuário	Desativar	Motivo	Transaction Time
1418751704	2014/12/16 15:41:44	2014/12/16 15:42:41	Bolo c/ Recheio	Bolos - Linha 2	FREDDIE	YP-49	Administrator	2014/12/16 15:41:24	Administrator		Subgrupo Desativado	2014/12/16 15:42:41
1418751704	2014/12/16 15:41:44	2014/12/16 15:41:44	Bolo c/ Recheio	Bolos - Linha 2	FREDDIE	YP-49	Administrator	2014/12/16 15:41:24	Administrator			2014/12/16 15:41:44
1418750813	2014/12/16 15:26:53	2014/12/16 15:27:39	Bolo c/ Cobertura	Bolos - Linha 2	FREDDIE	BP-60	Administrator	2014/12/16 15:26:21	Administrator		Erro de digitação	2014/12/16 15:27:39
1418750813	2014/12/16 15:26:53	2014/12/16 15:26:53	Bolo c/ Cobertura	Bolos - Linha 2	FREDDIE	BP-60	Operador	2014/12/16 15:26:21	Operador			2014/12/16 15:26:53
1335362238	2012/04/25 10:56:09	2014/12/16 15:23:32	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrator	2012/01/31 07:00:00	Administrator		Erro de digitação	2014/12/16 15:23:32
1335362238	2012/04/25 10:56:09	2014/12/16 16:00:28	Bolo c/ Cobertura	Bolos - Linha 2	SLOOP-D630	BP-55	Administrator	2012/01/31 07:00:00	Administrator	Excluir	Excluir Subgrupo	2014/12/16 15:23:32



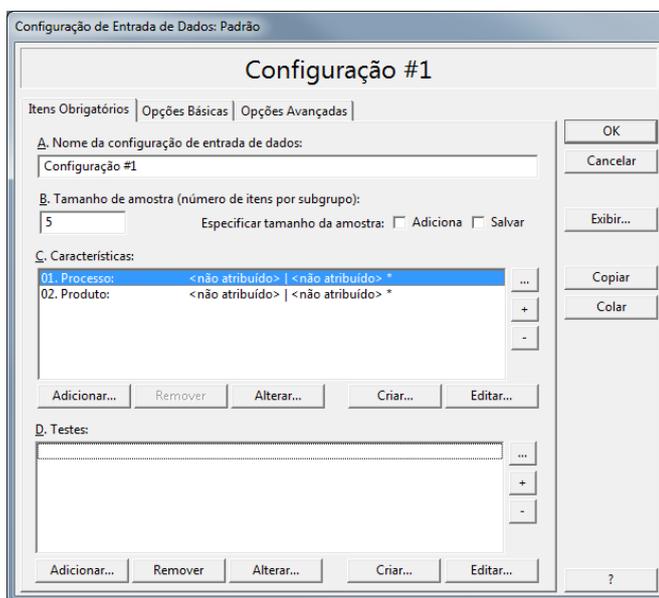
- f. Utilização de sistema operacional de checagens para aplicar sequências de etapas e eventos, conforme o caso.

As operações de coleta de dados do *InfinityQS ProFicient* são geridas por meio de uma sequência bem definida de passos, determinados pelo administrador do projeto. Essas etapas limitam as funções e as responsabilidades dos operadores. Além disso, as violações de controle de processo e eventos são gerenciadas por meio de uma sequência controlada de medidas para garantir o bom cumprimento do evento.

➤ **Início - Configurações Necessárias no Sistema**

Dentro de um projeto do *InfinityQS*, uma Configuração de Entrada de Dados define o **Procedimento de Entrada de Dados** ou as etapas tomadas por um operador para inserir dados. Esta configuração direciona a sequência e frequência da coleta de dados.

1. No projeto clique em **Entrada de dados | Novo | Padrão**. A janela **Configuração de Entrada de Dados** será exibida. Observe que a janela possui três abas: **Itens Obrigatórios**, **Opções Básicas** e **Opções Avançadas**.

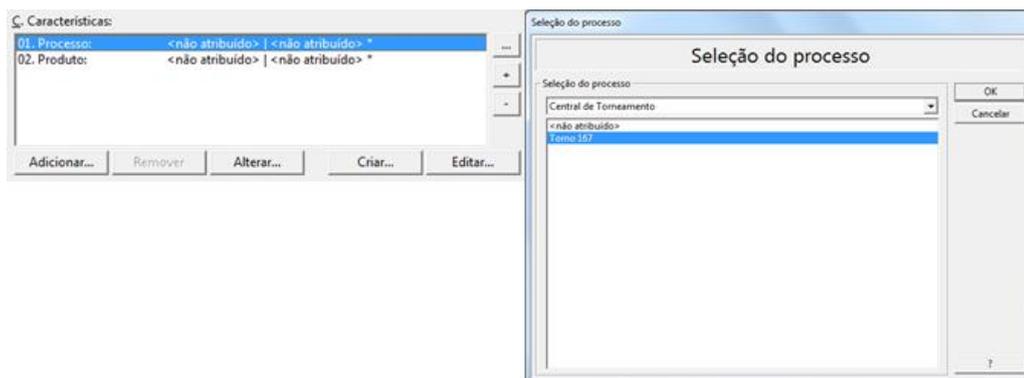


Configurando a Aba Itens Obrigatórios

Todos os campos devem ser especificados. Os usuários devem fornecer um nome da Configuração de Entrada de Dados, o Tamanho da Amostra, o Produto, o Processo e pelo menos um Teste. Todos os ajustes e/ou seleções restantes são opcionais e servem para fazer com que os esforços para o levantamento de dados sejam mais fáceis e os menores possíveis, acrescentando informações relevantes.

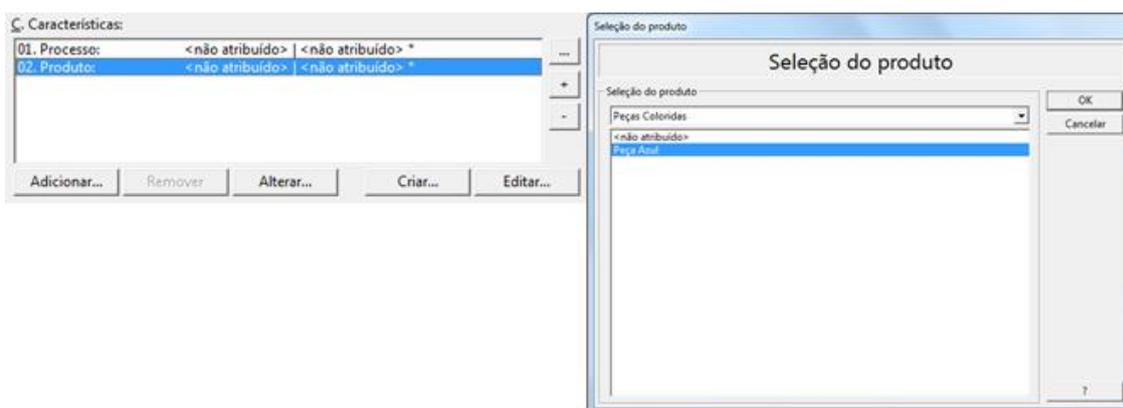
- *Seção Características*

Selecione a opção **01.Processo** e clique no botão **ALTERAR** para abrir a janela **Seleção do Processo**. Nesta janela, qualquer processo no banco de dados pode ser selecionado.



Opcionalmente, o usuário pode configurar as propriedades para permitir que a seleção do processo ocorra durante a entrada de dados. Clique no botão , para acessar a janela **Propriedades**. Por exemplo, digamos que um operador troque frequentemente de processo durante a fabricação de um produto. Neste caso, uma Seleção de Processo está disponível para permitir que o operador escolha ou re-selecione um Processo cada vez que ele fizer a entrada dados.

Selecione a opção **02.Produto** e clique no botão **ALTERAR** para abrir a janela **Seleção de Produto**. Nesta janela, qualquer produto no banco de dados pode ser selecionado.

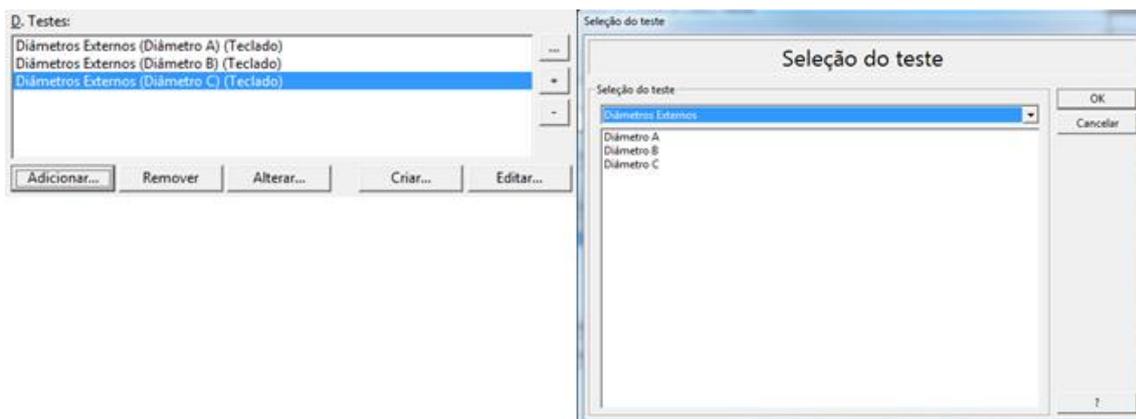


Opcionalmente, o usuário pode configurar as propriedades para permitir que a seleção do produto ocorra durante a entrada de dados. Clique no botão , para acessar a janela **Propriedades**. Por exemplo, digamos que um operador encontre frequentes mudanças do produto em suas máquinas. Neste caso, uma Seleção de Produto está disponível para permitir que o operador escolha ou re-selecione um Produto cada vez que ele fizer a entrada dados.

- **Seção Testes**

Pelo menos um **teste** deve ser especificado na Configuração da Entrada de Dados.

Clicando no botão **ADICIONAR** na seção Teste, é aberta a janela **Seleção do Teste**. Nesta janela, qualquer teste no Banco de Dados pode ser selecionado.



- *Sequência de Testes*

Testes selecionados podem ser movidos para cima ou para baixo na lista de testes utilizando os botões **+** e **-**. A sequência configurada na entrada de dados será a mesma sequência que o operador utilizará ao realizar o registro.

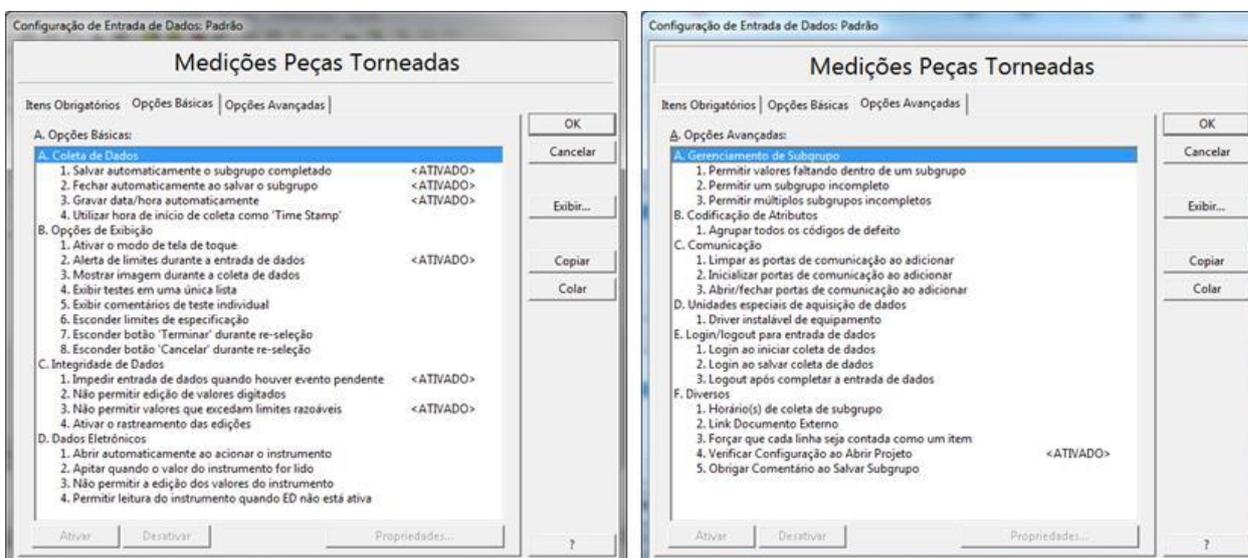
- *Características Opcionais*

Na aba Itens **Obrigatórios**, características podem ser adicionadas, removidas, criadas, editadas e configuradas.

Clique no botão **ADICIONAR** e selecione a característica desejada.

Configurando as Abas Opções Básicas e Opções Avançadas

Fornecem uma série de opções de configurações para a etapa de coleta de dados.

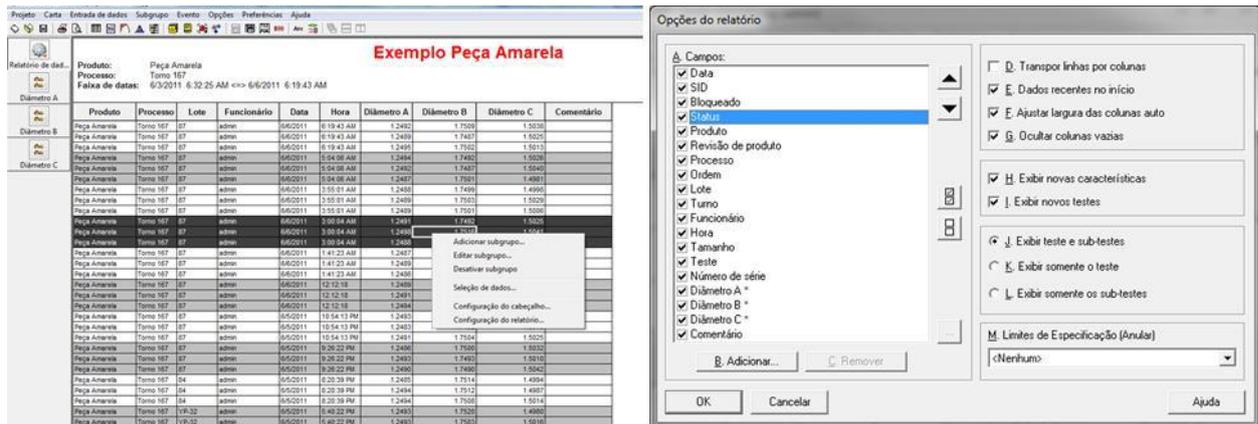


Quando terminar as configurações, clique no botão **OK**.

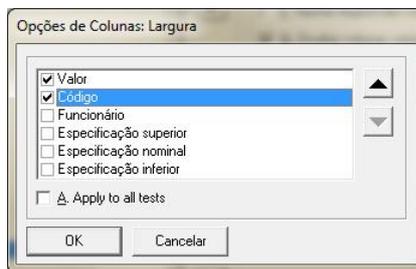
Outras Configurações

Quando um projeto for configurado para registrar subgrupos incompletos onde mais de um funcionário pode participar do registro ou quando diferentes funcionários podem editar um registro, é indicado realizar a seguinte configuração no Relatório de Dados:

1. Selecione o Relatório de Dados desejado, clique com o botão direito na tela, selecione a opção **Seleção de dados**, a janela **Opções do relatório** abrirá.



2. Na janela **Opções do relatório**, selecione um teste e clique nas reticências (...). A janela **Opções de Colunas: Largura** abrirá.



3. Na janela **Opções de Colunas: Largura** selecione a opção **Funcionário**. Repita este procedimento para todos os testes que desejar fazer esta configuração, ou habilite a opção **Aplicar para todos os testes**.

Com esta configuração, o Relatório de Dados irá mostrar uma nova coluna **Funcionário**, que trará o nome do funcionário que realizou ou editou a coleta para cada teste individualmente.

Lote	Funcionário	Data	Hora	Tamanho	Teste	Turno	Comprimento	Funcionário	Largura	Funcionário	Altura	Funcionário
BP-55	John	31/01/2012	05:00:00	3	1	Turno 2	82,5000	Sam Taft	15,0000	John	14,9850	Administrato
BP-55	John	31/01/2012	05:00:00	3	2	Turno 2	82,4900	Sam Taft	14,9900	John	14,9850	Administrato
BP-55	John	31/01/2012	05:00:00	3	3	Turno 2	82,3900	Sam Taft	15,0000	John	15,0040	Administrato
BP-56	Administrato	31/01/2012	04:00:00	3	1	Turno 2			15,0150	Administrato		
BP-56	Administrato	31/01/2012	04:00:00	3	2	Turno 2			15,0150	Administrato		
BP-56	Administrato	31/01/2012	04:00:00	3	3	Turno 2			15,0050	Administrato		
BP-56	Administrato	31/01/2012	03:00:00	3	1	Turno 2	82,5750	Administrato				
BP-56	Administrato	31/01/2012	03:00:00	3	2	Turno 2	82,5750	Administrato				
BP-56	Administrato	31/01/2012	03:00:00	3	3	Turno 2	82,5750	Administrato				
BP-56	Administrato	31/01/2012	02:00:00	3	1	Turno 2					15,0150	Administrato
BP-56	Administrato	31/01/2012	02:00:00	3	2	Turno 2					15,0050	Administrato
BP-56	Administrato	31/01/2012	02:00:00	3	3	Turno 2					15,0050	Administrato

O *Dynamic Scheduler* é outra ferramenta do *InfinityQS* que funciona como um “lembrete” para o operador, monitorando o horário que as medições devem ser realizadas. Porém, mais do que um lembrete, esta ferramenta funciona como um “supervisor”, monitorando, tomando ações, registrando eventos e exigindo causas atribuíveis quando o limite de tempo estabelecido para uma amostragem exceder.

O *Dynamic Scheduler* notifica o operador da estação de trabalho quando um subgrupo deve ser coletado, baseado nas configurações de amostragem.



➤ **Fim**

- g. Uso de checagem de autoridade para garantir que somente pessoas autorizadas utilizem o sistema, assinem eletronicamente um registro, tenham acesso à operação de entrada de informações no sistema, alterem um registro via dispositivos ou manualmente.

O sistema *InfinityQS* mantém uma lista de usuários, funções e permissões de acesso em um banco de dados centralizado. A autenticação do usuário é fornecida por uma combinação de login e senha que ficam mantidos neste banco de dados.

- Criptografia 128-bits utilizada para todas as senhas;
- Requisitos de complexidade de senhas impedem o uso de senhas “fracas”;
- Função que impede o envelhecimento de senha, forçando os usuários a mudar em um período de tempo especificado;
- Inibição de contas inativas, impede contas mortas de serem reutilizadas após um período de tempo específico;
- Bloqueio de conta automático garante proteção contra o uso não autorizado;
- *Logout* automático após um período de tempo inativo força um novo *login* para o usuário continuar o acesso.

➤ **Início - Configurações Necessárias no Sistema**

Utilizando configurações de senha, configurações de contas de usuário e rastreabilidade, pode-se assegurar que os dados do *ProFicient* não serão acessados ou modificados por usuários não autorizados.

Editando as Políticas de Segurança

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.

Configuração de Senha

- *Usar o Sign In automático do Windows*. Ativando esta opção, o *ProFicient* automaticamente é iniciado, logando com o usuário corrente do Windows e conferindo a senha do Windows com a senha armazenada no banco de dados do *ProFicient*. Sign In automático pode ser utilizado com autenticação do Windows ou LDAP, como descrito abaixo.
- *Usar autenticação do Windows*. Em vez do *ProFicient* ser iniciado automaticamente, esta opção faz com que a tela de login seja exibida com a inclusão do nome do domínio, e o operador terá que digitar o usuário e senha do Windows.
- Combinando a autenticação do Windows com o Sign In automático, pode-se pular a tela de login do usuário, sendo utilizada no lugar, a autenticação com o usuário do Windows de domínio.

- *Usar autenticação LDAP.* Similar a autenticação do Windows acima, esta opção faz com que a tela de login seja exibida com a inclusão do nome do domínio, e o operador terá que digitar o usuário e senha do Windows.
Combinando a autenticação LDAP com o Sign In automático, pode-se pular a tela de login do usuário, sendo utilizada no lugar, a autenticação com o usuário do Windows de domínio.
- *Máscara de Login.* Quando ativado, o ProFicient irá substituir cada caractere do login por um asterisco (*) durante a digitação do login.
- *Tamanho mínimo de senha.* Esta opção estabelece o número mínimo de caracteres para todas as senhas do ProFicient.
- *Idade mínima de senha.* Esta opção estabelece o tempo mínimo que deve ser aguardado antes que o usuário possa modificar a senha. **OBS:** Se esta opção for ativada, todos os usuários serão forçados a especificar uma senha única durante seu primeiro acesso no sistema.
- *Idade máxima de senha.* Esta opção estabelece o tempo máximo que pode ser aguardado antes que o usuário realize a modificação da senha. **OBS:** Se esta opção for ativada, todos os usuários serão forçados a especificar uma senha única durante seu primeiro acesso no sistema.
- *Notificação avançada de expiração de senha.* Esta opção estabelece quando o ProFicient irá iniciar os avisos de que a senha precisa ser alterada.
- *Proibir reciclar senhas durante.* Esta opção previne que o usuário reutilizem senhas anteriores por um determinado número de dias.
- *Senhas requerem números e letras.* Quando ativada, o ProFicient requer que as senhas criadas possuam obrigatoriamente números e letras.

Bloqueio de Conta

- *Conta ociosa: bloquear se ociosa por.* Esta opção bloqueia a conta que estiver ociosa durante um determinado período de tempo até que um usuário administrador a desbloqueie.
- *Erros de login: bloquear se ocorrerem mais de.* Esta opção bloqueia a conta na qual o usuário tiver realizado determinado número de tentativas falhas de login até que determinado tempo tenha transcorrido (**limpar contagem de erros após**), ou até um usuário administrador desbloquear a conta.
- *Limpar contagem de erros após.* Por padrão, a contagem de erros durante as tentativas de login é definida como zero após a realização do login com sucesso, mas pode-se também configurar o ProFicient para definir para zero após determinado número de minutos de inatividade.
- *Se a contagem for excedida: desbloquear conta após.* Esta opção previne o acesso do usuário a partir de uma conta que tenha sido bloqueada após determinada quantidade de tentativas falhas de login por um determinado número de minutos.

Logs de Acesso

- *Criar log de acesso dos usuários.* Quando ativada, o ProFicient captura cada login realizado com sucesso ao banco de dados e armazena esta informação na tabela *Log de Acesso (ACC_LOG)*.
- *Criar log de violações de acesso.* Quando ativada, o ProFicient captura cada tentativa falha de login e armazena esta informação na tabela *Log de Falha de Acesso (ACC_FAIL)*.

Atividade da conta

- *Fazer logout se inativo por.* Esta opção realiza o logout da conta que estiver inativa por um determinado número de minutos, sendo solicitada novamente a realização do login para que o acesso continue.

Rastreabilidade no banco de dados

- *Habilitar rastreabilidade de banco de dados.* Quando ativada, todas as modificações serão registradas nas tabelas de rastreabilidade do ProFicient.
- *Habilitar rastreabilidade de motivo de mudança.* Quando ativada, será solicitado ao usuário o registro de um motivo para a realização da alteração.

Login/logout para coleta de dados

- *Login ao iniciar coleta de dados.* Quando ativada, o usuário terá que realizar o login antes de iniciar uma entrada de dados.
- *Login ao salvar coleta de dados.* Quando ativada, após inserir os dados na tela de entrada de dados, o usuário terá que realizar o login antes que os dados sejam salvos no banco de dados.
- *Logout após completar a coleta de dados.* Quando ativada, é realizado automaticamente o logout do usuário após o subgrupo ser salvo.
- *Login antes de digitar uma nota de evento.* Quando ativada, o usuário terá que realizar o login antes de digitar uma nota no evento.
- *Login antes de salvar uma nota de evento.* Quando ativada, após o usuário digitar uma nota no evento, o usuário terá que realizar o login antes que a nota seja salva no banco de dados.
- *Login antes de digitar um comentário de subgrupo.* Quando ativada, o usuário terá que realizar o login antes de digitar um comentário de subgrupo.
- *Login antes de salvar um comentário de subgrupo.* Quando ativada, após o usuário digitar um comentário no subgrupo, o usuário terá que realizar o login antes que o comentário seja salvo no banco de dados.

➤ Fim

- h. A utilização de controles de dispositivo para determinar, se apropriado, a validade da fonte de entrada de dados ou instrução operacional.

Cada teste em um plano de coleta é configurado para aceitar dados de uma fonte específica. Requisitos adicionais podem ser configurados para requerer um tipo de instrumento específico, modelo ou *ID*. Cada dado coletado pode incluir o rastreamento do ID do instrumento utilizado. Requisitos de entrada podem ser configurados para a proteção contra a entrada de dados “sem sentido”. Essa função auxilia o sistema a prevenir erros claros de entrada de dados.

➤ Início - Configurações Necessárias no Sistema

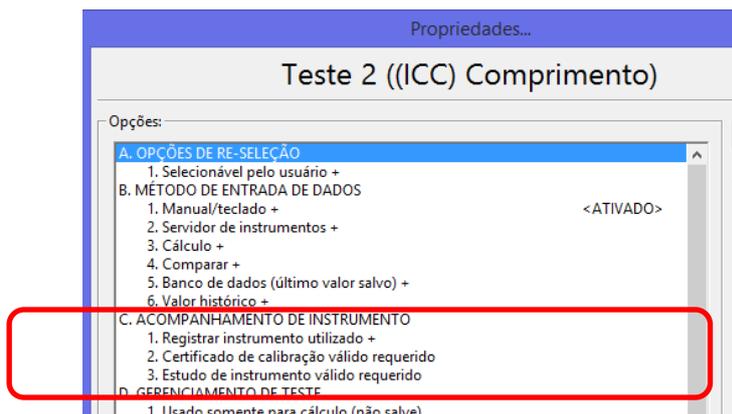
Antes que o *InfinityQS* possa realizar qualquer função analítica, primeiro os dados precisam ser escritos no banco de dados. O sistema permite uma série de opções para escrever os dados no banco. Abaixo se encontra uma lista das possibilidades.

- Entrada de dados manual
- Entrada de dados por meio de cálculos
- Integração com instrumentos e dispositivos de medição
- Recuperação de dados salvos previamente no banco a fim de utilizá-los nos próximos cálculos
- Importação de dados utilizando o *InfinityQS Import Utility*
- Transferência de dados de arquivos texto por meio do *Buffer File driver*
- Transferência de dados a partir de outros bancos de dados, aplicativos e supervisórios utilizando o *Data Management System (DMS)* ou o *Dynamic Data Exchange (DDE)*

- Utilização de licença de *software* customizado para desenvolver sua própria interface de entrada de dados
- Escrever diretamente os dados nas tabelas do banco por meio de uma customização à parte

Integração Dispositivos de Medição

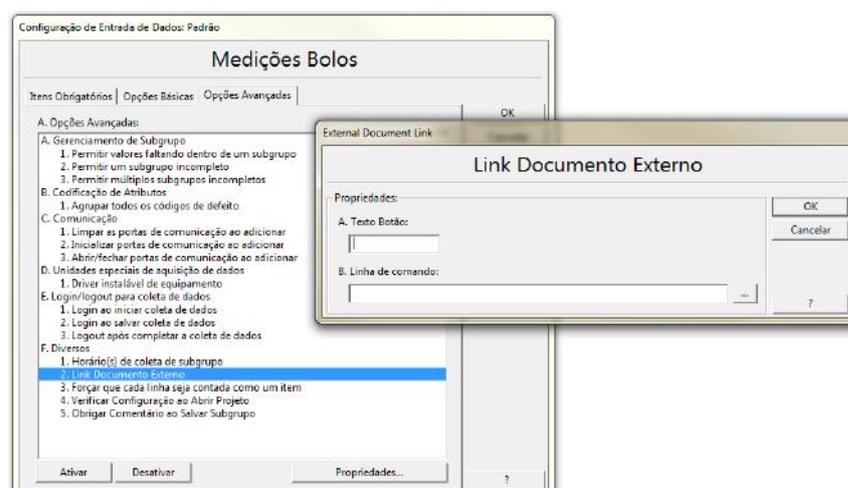
O *InfinityQS* possui uma interface de configuração de instrumentos chamada **Servidor de Instrumentos (Gage Server)**. Por meio deste utilitário, é possível configurar dispositivos de medição para permitir a transferência de dados diretamente do dispositivo para o banco de dados. A identificação do instrumento utilizado em cada registro também pode ser ativada.



Instrução Operacional – Link para Documento Externo durante a Coleta de Dados.

O *InfinityQS* possibilita a criação de um botão para ficar disponível na tela de coleta de dados, assim pode ser configurado um arquivo, um endereço web, um programa, entre outros para ficar disponível no momento da coleta de dados.

1. Na Configuração de Entrada de Dados, localize a aba **Opções Avançadas**. Na seção **Diversos**, ative a opção **2. Link Documento Externo**. A janela **Link Documento Externo** abrirá.



2. Na janela **Link Documento Externo** faça as configurações necessárias.
 - No campo **Texto Botão** configure o nome do botão.
 - No campo **Linha de comando** localize o documento externo que deve ser configurado.
3. Na próxima coleta de dados o botão configurado irá aparecer na tela de coleta de dados.

Instrução Operacional - Imagem durante a Coleta de Dados

1. No *Database Manager*, localize a tabela *Produto / Teste – Informação [PART_TEST]*.

51	Produto - Definição (PART_DEF)	10	F_VAR3
52	Produto - Grupo (PART_GRP)	11	F_VAR4
53	Produto - Número de série (PART_SN)	12	F_STR1
54	Produto - Revisão (PART_REV)	13	F_STR2
55	Produto / Teste - Informação (PART_TEST)	14	F_USER
56	Rede (NET_INF)	15	F_DSBL
57	Regra de alarme - Definição (RULE_DEF)	16	F_RFC
58	Regra de alarme (ALR_RULE)	17	F_TRTM

2. Execute duplo clique sobre a linha referente à tabela *Produto / Teste- Informação*. A janela **Produto / Teste – Informação (PART_TEST)** será exibida.
3. Abra a janela de adição **Produto / Teste- Informação: Adicionar**.
4. No campo **Produto**, clique no botão reticências (...), e na tela **Produto – Item: Selecionar** selecione o produto desejado e clique **OK**.
5. No campo **Teste**, clique no botão reticências (...), e na tela **Teste – Item: Selecionar** selecione o teste desejado e clique **OK**.
6. Na tela **Produto/Teste- Informação: Adicionar**, localize a seção **Informação**.

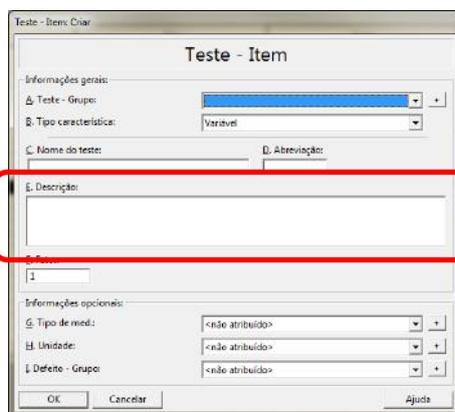


- No campo **Tipo de valor**, clique na lista de seleção e selecione a opção **Gráfico**.
- (Opcional) No campo **Descrição**, digite uma descrição para este Gráfico.
- No campo **Arquivo**, clique no botão reticências (...) e navegue até o gráfico (imagem) desejado.

Na tela de coleta de dados, o *SPC MI* irá exibir a imagem definida para a combinação produto/teste.

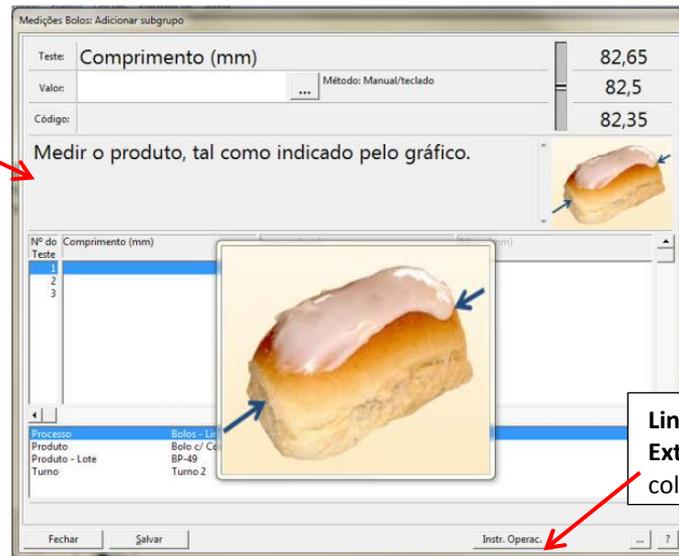
Instrução Operacional - Instruções durante a Coleta de Dados

1. Dentro do *Database Manager*, na janela contendo as tabelas, localize e execute duplo clique na tabela *Teste - Item [TEST_DAT]* para exibi-la.
2. Adicione ou edite um teste específico e preencha o campo **Descrição**.



As informações do campo **Descrição** aparecem como instrução durante a coleta de dados para o teste configurado.

Instrução durante a coleta



Teste: Comprimento (mm) 82,65
 Valor: 82,5 Método: Manual/teclado
 Código: 82,35

Medir o produto, tal como indicado pelo gráfico.

Nº do Teste	Comprimento (mm)
1	
2	
3	

Processo: Bolos e Bolo
 Produto: Bolo c/ C Bolo
 Produto - Lote: BP-49
 Turno: Turno 2

Fechar Salvar Instr. Operac. ?

Imagem durante a coleta

Link para Documento Externo durante a coleta

➤ **Fim**

§ 11.50 Manifestações de assinatura

- a. Registros eletrônicos assinados devem conter informações associadas à assinatura indicando claramente os seguintes itens:
1. O nome impresso do assinante;
 2. O dia e hora em que a assinatura foi realizada; e
 3. O significado (assim como a revisão, aprovação, responsabilidade, ou autoria) associado à assinatura.

Os aplicativos da *InfinityQS*[®] suportam dois tipos de assinatura. Ambos são baseados em uma autenticação de usuário por uma única combinação de login e senha mantidos dentro da base de dados centralizada.

Todos os registros de motivo de troca fornecem as seguintes informações:

- Nome do funcionário;
- Data/hora da assinatura;
- Código do motivo de mudança;
- Comentários.

Todos os registros de eventos do processo fornecem as seguintes informações:

- Nome do funcionário (evento);
- Data/hora do evento;
- Tipo de evento;
- Nome do funcionário (Causa atribuível);
- Data/hora da causa atribuível;
- Código da causa atribuível;
- Nome do funcionário (ação corretiva);
- Data/hora da ação corretiva;
- Código da ação corretiva;
- Comentários.

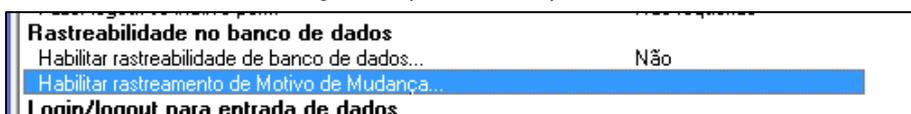
➤ **Início - Configurações Necessárias no Sistema**

O acesso ao banco de dados é realizado através de uma senha e *login* individual com permissões específicas para cada usuário.

Através da política de segurança do banco de dados é possível configurar os logs de acesso que obrigam a assinatura do funcionário ao iniciar ou salvar um registro, evento ou um comentário.

Editando as Políticas de Segurança

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.
3. Na seção **Rastreabilidade no banco de dados**, dê um duplo clique na opção **Habilitar rastreamento de Motivo de Mudança** e clique em **Sim** para habilitá-la.

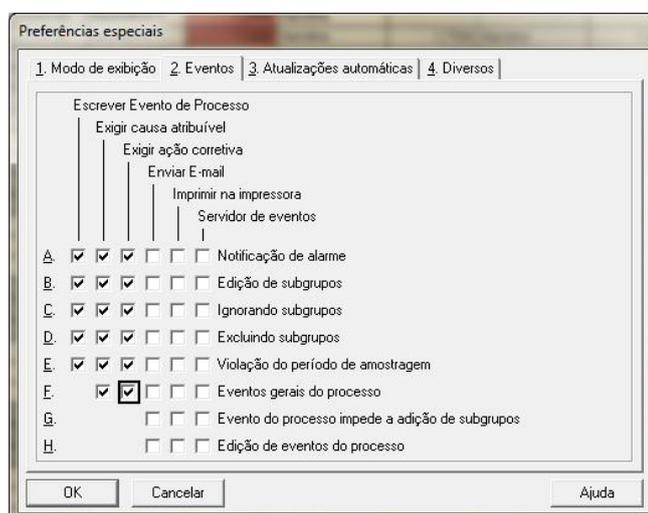


Com a opção de rastrear os motivos das modificações dos registros, é solicitado que o usuário insira uma explicação/motivo para cada modificação realizada, considerado nomes de produtos, processos, testes, limites de controle, limites de especificação, valores de teste, funcionários, e todas as outras informações, e também fornece a habilidade de gerar relatórios com os resumos das modificações.

4. Configure a seção **Login/logout para coleta de dados**.

Configurando o Projeto

1. A partir da barra de menu do projeto do *ProFicient SPC MI*, clique em **Preferências | Projeto | Especial**, localize a aba **2.Eventos**.
2. Na aba **2.Eventos** habilite as opções para a rastreabilidade da edição dos registros.



➤ **Fim**

- b. Os itens identificados nos parágrafos (a)1, (a)2 e (a)3, desta seção devem estar sujeitos aos mesmos controles como registros eletrônicos e devem ser incluídos como parte de qualquer formato legível de registro eletrônico (como visualização eletrônica ou impresso).

Os pacotes da *InfinityQS*® inclui um pacote compreensivo de registros para fornecer esta informação em formato legível para pessoas. Estes registros podem ser vistos em tela ou em versões para impressão.

➤ Início - Configurações Necessárias no Sistema

Visualizando os Registros

Após a configuração do *Database Manager* e do *ProFicient SPC MI*, conforme o item anterior, você garante a rastreabilidade do registro e edição de coleta de dados. Dessa maneira ficará registrado o horário do registro, o funcionário responsável por responder cada teste, o motivo de alteração do registro assim como o horário da alteração e o responsável pela modificação.

Registro da Coleta

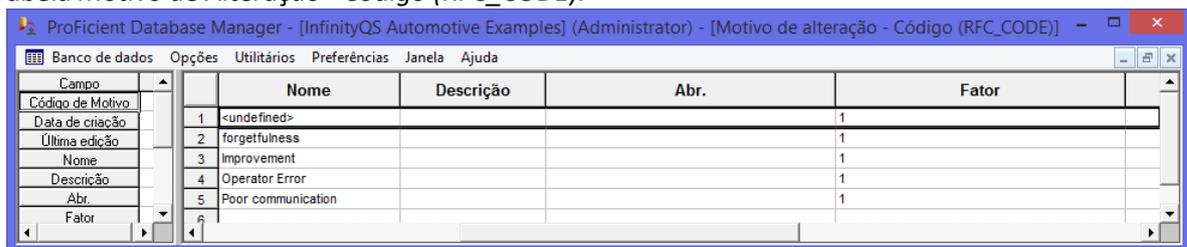
Produto: Peça Amarela
 Processo: Torno 167 (Manutenção)
 Faixa de datas: 08/02/2010 00:29:34 <=> 16/03/2015 11:01:54

Produto	Processo	Turno	Funcionário	Data	Hora	Dispositivo	Diâmetro A	Funcionário	Diâmetro B	Funcionário	Diâmetro C	Funcionário	Comentário
Peça Amarela	Torno 167	A	Karolina	16/03/2015	11:01:54	dispositivo-5	1,2500	Karolina	1,7490	joao	1,5000	Pedro	
Peça Amarela	Torno 167	A	Karolina	16/03/2015	11:01:54	dispositivo-2	1,2500	Karolina	1,7500	joao	1,4980	Karolina	
Peça Amarela	Torno 167	A	Karolina	16/03/2015	11:01:54	dispositivo-4	1,2490	Karolina	1,7510	joao	1,5010	Pedro	
Peça Amarela	Torno 167	A	Karolina	13/02/2015	12:01:20	dispositivo-1	1,2400	Karolina	1,7500	Karolina	1,5000	Karolina	Coleta realizada com supervisão *
Peça Amarela	Torno 167	A	Karolina	13/02/2015	12:01:20	dispositivo-1	1,2500	Karolina	1,7500	Karolina	1,5000	Karolina	Coleta realizada com supervisão *
Peça Amarela	Torno 167	A	Karolina	13/02/2015	12:01:20	dispositivo-1	1,2500	Karolina	1,7500	Karolina	1,5000	Karolina	Coleta realizada com supervisão *

Registro de Motivo de Modificação

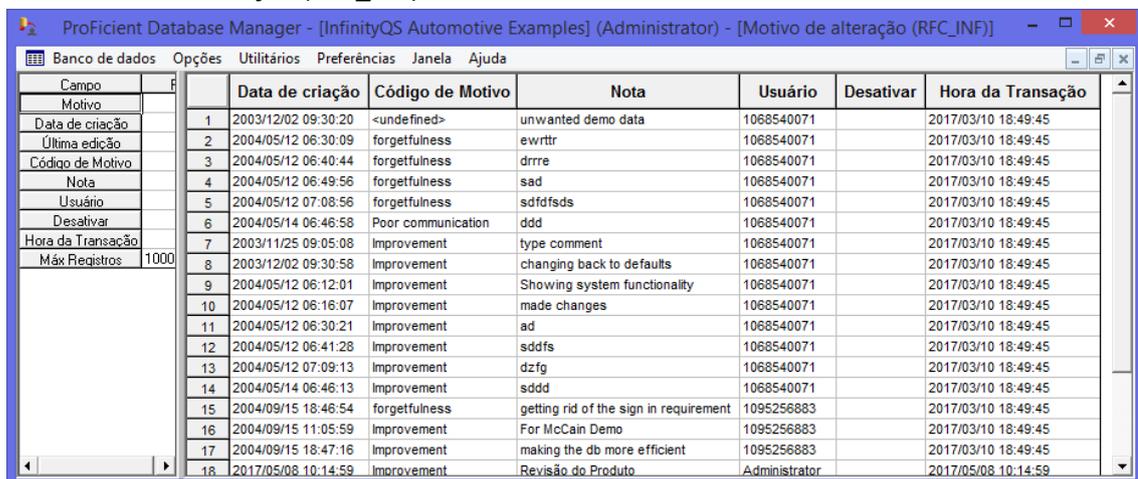
A partir do *Database Manager* é possível visualizar relatórios com as listas dos códigos de motivos de alterações, assim como a descrição de cada motivo associado inserida pelo usuário, e a tabela

Tabela *Motivo de Alteração - Código (RFC_CODE)*:



Campo	Nome	Descrição	Abr.	Fator
Código de Motivo	1	<undefined>		1
Data de criação	2	forgetfulness		1
Última edição	3	Improvement		1
Nome	4	Operator Error		1
Descrição	5	Poor communication		1
Abr.	6			
Fator				

Tabela *Motivo de Alteração (RFC_INF)*:

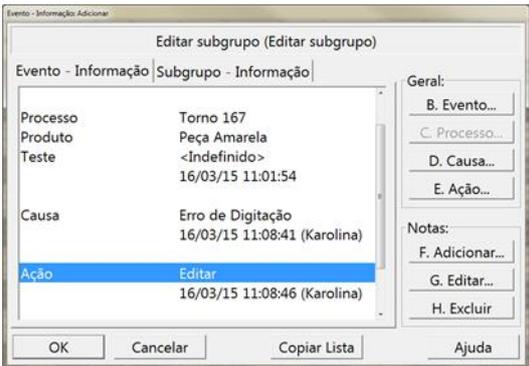


Campo	Data de criação	Código de Motivo	Nota	Usuário	Desativar	Hora da Transação
Motivo	1	<undefined>	unwanted demo data	1068540071		2017/03/10 18:49:45
Data de criação	2	forgetfulness	ewrtrr	1068540071		2017/03/10 18:49:45
Última edição	3	forgetfulness	drerre	1068540071		2017/03/10 18:49:45
Código de Motivo	4	forgetfulness	sad	1068540071		2017/03/10 18:49:45
Nota	5	forgetfulness	sdfdsfs	1068540071		2017/03/10 18:49:45
Usuário	6	Poor communication	ddd	1068540071		2017/03/10 18:49:45
Desativar	7	Improvement	type comment	1068540071		2017/03/10 18:49:45
Hora da Transação	8	Improvement	changing back to defaults	1068540071		2017/03/10 18:49:45
Máx Registros	9	Improvement	Showing system functionality	1068540071		2017/03/10 18:49:45
	10	Improvement	made changes	1068540071		2017/03/10 18:49:45
	11	Improvement	ad	1068540071		2017/03/10 18:49:45
	12	Improvement	sdfs	1068540071		2017/03/10 18:49:45
	13	Improvement	dzfg	1068540071		2017/03/10 18:49:45
	14	Improvement	sddd	1068540071		2017/03/10 18:49:45
	15	forgetfulness	getting rid of the sign in requirement	1095256883		2017/03/10 18:49:45
	16	Improvement	For McCain Demo	1095256883		2017/03/10 18:49:45
	17	Improvement	making the db more efficient	1095256883		2017/03/10 18:49:45
	18	Improvement	Revisão do Produto	Administrator		2017/05/08 10:14:59

Tabela referente ao item modificado com o respectivo Motivo associado:

	Data de criação	Última edição	Nome	Usuário	Desativar	Motivo	Hora da Transação
116	2002/02/07 19:39:36	2006/04/03 12:07:33	1.00 Block				2017/03/10 18:49:49
117	2002/02/07 19:39:47	2006/04/03 10:46:36	2.00 Block				2017/03/10 18:49:49 *
118	2002/02/07 19:39:47	2017/05/08 10:14:59	2.00 Block R1	Administrator		Revisão do Produto	2017/05/08 10:14:59
119	2002/02/07 19:39:50	2006/04/03 10:46:48	3.00 Block				2017/03/10 18:49:49

Registro de Evento de Processo



Produto:	Peça Amarela, Peça Azul	
Processo:	Torno 167 (Manutenção), Torno 225 (Manutenção)	
Faixa de datas:	17/05/2010 15:03:38 <=> 16/03/2015 11:08:39	
16/03/2015 11:08:39	Editar subgrupo:	Editar subgrupo (Karolina)
16/03/2015 11:01:54	Processo:	Torno 167
	Produto:	Peça Amarela
	Turno:	A
	Funcionário:	Karolina
	Dispositivo:	dispositivo-2, dispositivo-4, dispositivo-5
16/03/2015 11:08:41	Causa:	Erro de Digitação (Karolina)
16/03/2015 11:08:46	Ação:	Editar (Karolina)

➤ **Fim**

§ 11.70 Links para registros/assinaturas.

Assinaturas eletrônicas e manuscritas executadas para arquivos eletrônicos devem estar conectadas às suas respectivas assinaturas eletrônicas para assegurar que as assinaturas não podem ser removidas, copiadas, ou então transferidas para a falsificação de um registro eletrônico.

Todos os registros do sistema *InfinityQS* estão conectados ao usuário que criou ou modificou o registro. A rastreabilidade de mudanças não pode ser excluída ou modificada de maneira alguma dos aplicativos certificados da *InfinityQS*®. O acesso aos registros por meio externo dos aplicativos do sistema são restritos apenas pela segurança da base de dados, que é de responsabilidade do cliente ou proprietário da base de dados.

Subparte C – Assinaturas Eletrônicas

§ 11.100 Requisitos Gerais

- a. Cada assinatura eletrônica deve ser única para cada indivíduo e não deve ser reusada por, ou reassinada para, ninguém.

Cada usuário do *InfinityQS* é identificado por um único identificador na base de dados e não pode ser visto, excluído ou removido, mas pode ser desabilitado para uso futuro. Estes identificadores únicos estão anexados a cada registro na base de dados, identificando o usuário que criou ou modificou o registro. Como uma medida de segurança, novos usuários são forçados a especificar uma senha única durante seu primeiro uso no sistema. Isto assegura que apenas os usuários, e mais ninguém (nem mesmo o administrador), saibam suas senhas.

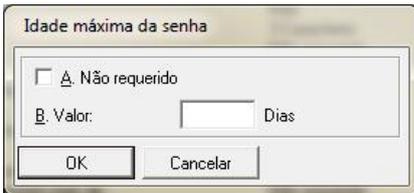
➤ **Início - Configurações Necessárias no Sistema**

Para que cada novo usuário seja forçado a especificar uma senha única durante seu primeiro uso no sistema é necessário configurar as políticas de segurança do banco de dados.

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.

Política de segurança	
Descrição	Valor
Configuração de senha	
Usar o Sign In automático do Windows...	Não
Usar autenticação do Windows...	Não
Usar a autenticação LDAP...	Não
Máscara de login...	Não
Tamanho mínimo da senha	3 Caracteres
Idade mínima da senha	Não requerido
Idade máxima da senha	Não requerido
Notificação avançada de expiração da senha	
Proibir reciclar senhas durante...	Não requerido
Senhas requerem números e letras...	Não
Bloqueio da conta	

- Na seção **Configuração de senha**, dê um duplo clique na opção **Idade máxima da senha** e digite o número máximo de dias para a troca da senha.



- Após esta configuração realizada, todos os usuários já criados, inclusive o administrador, e todos os usuários que serão criados, deverão alterar sua senha no seu primeiro acesso.

➤ **Fim**

§ 11.200 Componentes e controles da assinatura eletrônica.

a. Assinaturas eletrônicas que não são baseadas em biométricas devem:

- Empregar pelo menos dois diferentes componentes de identificação assim como um código identificador e senha.

Um *login* e uma senha são requeridos para obter acesso ao sistema *InfinityQS*. Estes dois itens identificam um único usuário do *InfinityQS*, e seu nome é subsequentemente associado a qualquer registro que seja feito pelo mesmo.

- Quando um indivíduo executa uma série de assinaturas durante um único acesso contínuo e controlado ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônica. Subsequentes assinaturas devem ser executadas usando pelo menos um dos componentes da assinatura eletrônica que é executável apenas por, e feito para ser usado pelo indivíduo.

Requisições adicionais para o *login* podem ser solicitadas. Isto inclui solicitar que o usuário faça o *login* antes de começar qualquer coleta de dados e/ou antes de salvar uma entrada de dados. Requisições automáticas de *logout* (forçando um subsequente *login*) podem ser implementadas com base em um tempo determinado de inatividade e realização de uma operação de entrada de dados. *Logins* múltiplos (até três) podem ser requisitados para a criação e realização de qualquer evento de processo.

- Quando um indivíduo executa um ou mais *logins* sem que seja durante um único período de acesso contínuo ao sistema, cada *login* deve ser executado usando todos os componentes da assinatura eletrônica.

Requisições automáticas de *logout* (forçando um subsequente *login*) podem ser implementadas com base no tempo de inatividade e realização de uma entrada de dados. Ambos *login* e senha são requisitados para re-acessar o sistema.

➤ **Início - Configurações Necessárias no Sistema**

O sistema permite que o último usuário logado seja lembrado nas assinaturas subsequentes, sendo necessário digitar somente a senha. Caso o acesso seja de outro usuário, ele permite alterar o usuário.



Para solicitar *login* e *logout* do usuário em situações diversas durante a coleta de dados é necessário configurar as políticas de segurança do banco de dados.

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.
3. Na seção **Login/logout para coleta de dados**, habilite as opções desejadas.

Login/logout para entrada de dados	
Login antes de iniciar entrada de dados...	Não
Login antes de salvar dados entrados...	Não
Logout após completar a entrada de dados...	Não
Entre no sistema antes de digitar uma nota de evento...	Não
Entre no sistema antes de salvar uma nota de evento...	Não
Entre no sistema antes de digitar um comentário de subgrupo...	Não
Entre no sistema antes de salvar um comentário de subgrupo...	Não

➤ **Fim**

2. Ser usadas apenas por seus proprietários verdadeiros; e

Medidas de segurança incorporadas ao sistema *InfinityQS* auxiliam a assegurar que uma assinatura eletrônica é usada apenas pelo seu verdadeiro autor. Estas medidas incluem envelhecimento de senha, reciclo de senha, bloqueio de conta inativa, bloqueio de re-tentativa e senha criptografada 128-bit. Treinamento de usuários com a segurança adequada e o uso de senhas é fundamental para a integridade de seu uso.

➤ **Início - Configurações Necessárias no Sistema**

As configurações de senha do usuário são configuradas nas políticas de segurança do banco de dados.

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.
3. Habilite as opções desejadas.

➤ **Fim**

3. Ser administradas e executadas para assegurar que tentativas de uso de uma assinatura eletrônica por outras pessoas que não o autor, requeiram a colaboração de dois ou mais indivíduos.

Apenas administradores do sistema *InfinityQS* com apropriados direitos de uso podem criar as senhas que garantem acesso ao sistema. Estas senhas devem ser modificadas pelos proprietários usuários em seu primeiro acesso ao mesmo.

- b. Assinaturas eletrônicas baseadas em biometrias devem ser concebidas para assegurar que elas não podem ser usadas por nenhuma outra pessoa a não ser os proprietários.

Dispositivos de biometria, como reconhecimento de impressão digital, scanner de retina e outros, podem ser incorporados como parte do sistema *InfinityQS*. Recomenda-se realizar testes prévios junto ao fabricante destes dispositivos para verificar a compatibilidade com o Sistema.

§ 11.300 Controles para senhas/códigos de identificação.

Pessoas que usam assinaturas eletrônicas baseadas no uso de códigos de identificação em combinação com senhas devem empregar controles para assegurar sua segurança e integridade. Tais controles devem incluir:

- a. Manter exclusividade de cada combinação de *login* e senha para que não seja possível duas pessoas terem a mesma combinação de acesso.

O *InfinityQS* mantém uma única combinação de *login* e senha associada exclusivamente para cada usuário do sistema. Estas combinações únicas identificam cada usuário individualmente, impedindo que seja possível duas pessoas acessarem com a mesma combinação. Todas as senhas dentro do sistema são criptografadas usando criptografia 128-bit. O tamanho de senha e sua complexidade (por exemplo com a opção de exigir caracteres com letras e números) são configuráveis no sistema.

- b. Assegurar que a emissão de códigos de identificação e senhas sejam periodicamente checados ou revisados (por exemplo para a mudança de senha envelhecida).

Todas as senhas devem ser trocadas imediatamente no primeiro acesso ao sistema pelo usuário. A função Envelhecimento de Senha exige que o usuário atualize a mesma a cada período de tempo (configurável no sistema). A função reciclagem de senha impede que um usuário reutilize uma senha antiga (configurável no sistema).

➤ **Início - Configurações Necessárias no Sistema**

As configurações de senha do usuário são configuradas nas políticas de segurança do banco de dados.

1. A partir da barra de menus do Database Manager, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.
3. Habilite as opções desejadas.

➤ **Fim**

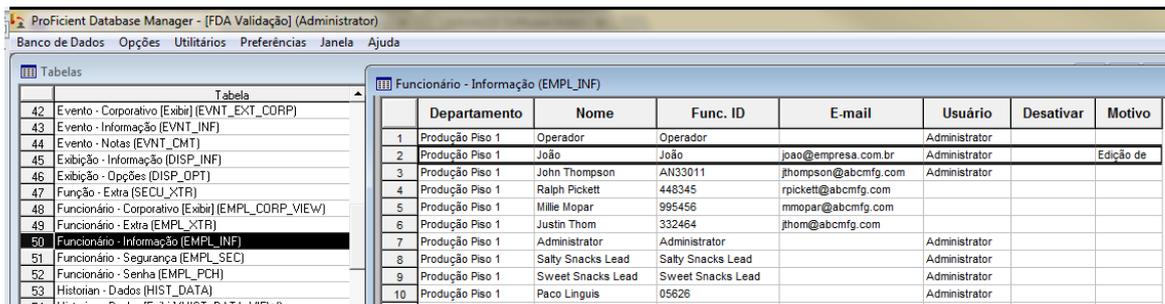
- c. Seguir os procedimentos de gerenciamento de perdas para eletronicamente desautorizar a perda, roubo, ou então fichas comprometidas, cartões, e outros dispositivos que suportam ou geram as informações de *login* e senha, e emitir substituições temporárias usando controles rigorosos adequados.

Usuários podem modificar suas senhas a qualquer momento que julgarem ser necessário por algum motivo. Administradores podem também bloquear o acesso a um usuário a qualquer momento, ou forçar o usuário a entrar uma nova senha para proteger a integridade do sistema.

➤ Início - Configurações Necessárias no Sistema

Administradores ou usuários que possuem a permissão de gerenciar funcionários podem alterar o acesso de outros funcionários.

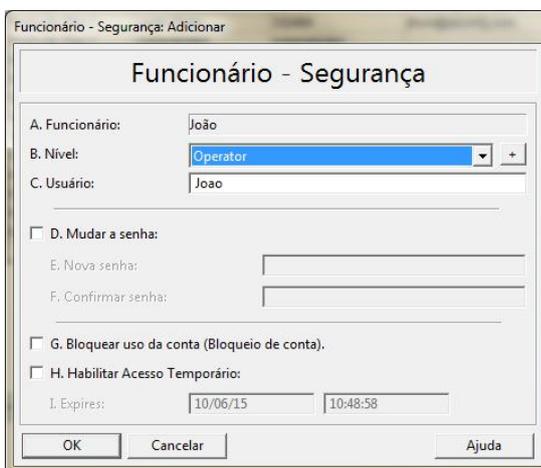
1. Dentro do *Database Manager*, na janela contendo as tabelas, localize e execute duplo clique na tabela *Funcionário – Informação (EMPL_INF)* para exibi-la. Ao abrir a tabela de Funcionário, é possível verificar todos os usuários cadastrados no banco de dados. Escolha o funcionário que deseja gerenciar.



Departamento	Nome	Func. ID	E-mail	Usuário	Desativar	Motivo
1	Operador	Operador		Administrator		
2	João	João	joao@empresa.com.br	Administrator		Edição de
3	John Thompson	AN33011	jthompson@abcmfg.com	Administrator		
4	Ralph Pickett	448345	rpickett@abcmfg.com			
5	Millie Mopar	995456	mmopar@abcmfg.com			
6	Justin Thom	332464	jthom@abcmfg.com			
7	Administrator	Administrator		Administrator		
8	Salty Snacks Lead	Salty Snacks Lead		Administrator		
9	Sweet Snacks Lead	Sweet Snacks Lead		Administrator		
10	Paco Linguis	05626		Administrator		

2. Na aba *Funcionário – Segurança: Adicionar* é possível realizar as seguintes configurações:

- Mudar a senha: forçar que o usuário altere a senha.
- Bloquear uso da conta: bloqueia a conta de acesso do usuário. Desmarcando esta opção o usuário volta a ter acesso ao InfinityQS.
- Habilitar acesso temporário: permite agendar um período para o acesso do usuário ao InfinityQS.



Alterando a Senha

Todo usuário pode modificar a senha no momento que julgar necessário.

1. Na tela *Login* do usuário, digite o usuário e a senha e depois clique no botão **MUDAR A SENHA**.



2. Na tela **Mudar a senha**, digite a nova senha e depois clique no botão **OK**. A senha será modificada.

➤ Fim

- d. Usar garantias de transação para prevenir uso não-autorizado de senhas ou *logins*, e para detectar e reportar de maneira imediata qualquer tentativa de acesso não autorizado à unidade de segurança do sistema, se apropriado, para o gerenciamento organizacional.

Todos os registros do sistema são mantidos em uma tabela de acesso dentro da base de dados do *InfinityQS*. Estas informações incluem Data/Hora de acesso, nome do computador de onde ocorreu o acesso, aplicativo para o qual o acesso foi concedido, usuário para o qual o acesso foi concedido e tipo de acesso concedido. Todos os registros de violação de acesso são mantidos em uma tabela de violação de acesso dentro da base de dados. Essa informação inclui:

- Data/Hora da tentativa de acesso;
- Nome do computador onde ocorreu a tentativa de acesso;
- Nome do *login* utilizado;
- Aplicativo utilizado para a tentativa de acesso;
- Razão para a tentativa de acesso ter sido rejeitada.

Códigos de falha de acesso incluem bloqueio de conta, eliminação de conta, número de tentativas excedido, privilégio inválido, *login* incorreto, senha incorreta.

➤ Início - Configurações Necessárias no Sistema

As configurações de bloqueio da conta são configuradas nas políticas de segurança do banco de dados.

1. A partir da barra de menus do *Database Manager*, clique em **Preferências | Política de Segurança**.
2. A tela **Política de segurança** será exibida.
3. Na seção **Bloqueio da conta**, habilite as opções desejadas.

Bloqueio da conta		Valor
Conta ociosa: bloquear se ociosa por...		Não requerido
Erros de login: bloquear se ocorrerem mais de...		Não requerido
Limpar contagem de erros após...		Não requerido
Se a contagem for excedida: desbloquear conta após...		Jamais

Rastreabilidade

Os registros de acesso ficam salvos na tabela *Log de acesso (ACC_LOG)* do *Database Manager*.

1. No *Database Manager*, localize a tabela *Log de acesso (ACC_LOG)* e execute duplo clique. A tabela de rastreabilidade será exibida.

Campo	Data de criação	Última edição	Cpu	Aplicação	Data/hora acesso	Código acesso	Usuário	
Log de acesso	14	2011/11/23 07:30:39	2011/11/23 07:30:39	SIMO-E6410	IDBM	2011/11/23 12:30:39	Login	Administrator
Data de criação	15	2011/11/23 07:30:32	2011/11/23 07:30:32	SIMO-E6410	IDBM	2011/11/23 12:30:32	Logout	Administrator
Última edição	16	2011/11/23 07:20:22	2011/11/23 07:20:22	SIMO-E6410	IDBM	2011/11/23 12:20:22	Login	Administrator
Cpu	17	2012/01/24 09:46:12	2012/01/24 09:46:12	SIMO-E6410	IDBM	2012/01/24 14:46:12	Login	Administrator
Aplicação	18	2011/11/23 07:12:58	2011/11/23 07:12:58	SIMO-E6410	IDBM	2011/11/23 12:12:58	Logout	Administrator
Data/hora acesso								

➤ Fim

- e. Testes iniciais ou periódicos de dispositivos, como tokens ou cartões, que carregam ou geram informações de códigos ou senhas que garantem a funcionalidade apropriada e que não tenha sido alterado de maneira não-autorizada.

Estes itens são externos ao Sistema *InfinityQS*, portanto, se forem implementados, devem ser testados com base nos procedimentos dos fornecedores.