



# Ministério da Fazenda

Serviço Federal de Processamento de Dados (SERPRO)

# *RLSL* (Rede Local Software Livre)



**Apresentador: Marcelo Rocha Rabelo de Andrade**

**Dezembro/2009 - v.04**

Serviço Federal de  
Processamento de Dados



Ministério  
da Fazenda



[www.serpro.gov.br](http://www.serpro.gov.br)



## Criação

O Serviço Federal de Processamento de Dados (SERPRO) é a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil. Foi criado pela Lei nº 4.516, de 1º de dezembro de 1964, para modernizar e dar agilidade a setores estratégicos da administração pública. É uma empresa vinculada ao Ministério da Fazenda e cresceu desenvolvendo programas e serviços que permitiram maior controle e transparência sobre a receita e os gastos públicos. Consolidou-se, ao longo desses anos, aprimorando tecnologias adotadas por diversos órgãos públicos federais, estaduais e municipais, e incorporadas à vida do cidadão brasileiro.

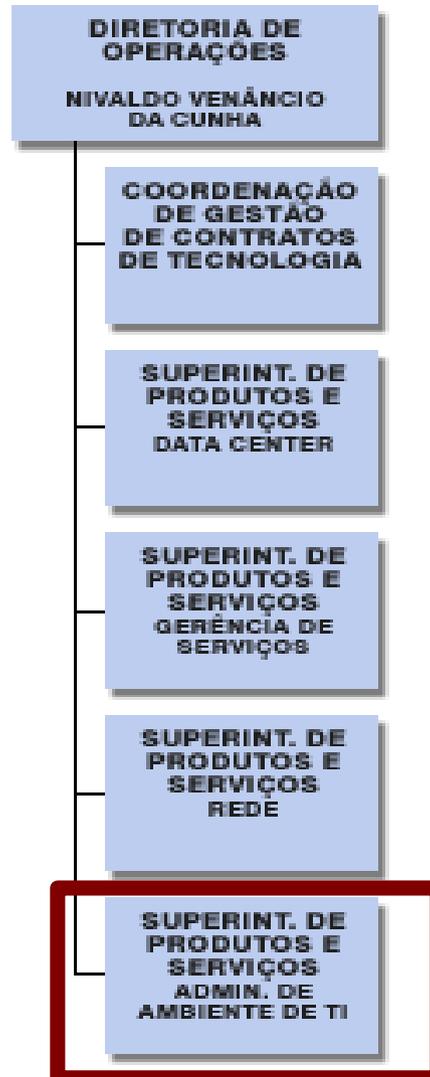


## Representações





## Diretoria de operações





## Histórico

- ◆ Estudos iniciados em 1999;
- ◆ Estruturação de Centros de Especialização na SUPTI;
- ◆ Adoção da suíte de escritório BOffice (Openoffice.org);
- ◆ Implantação de GNU/Linux nas estações de trabalho;
- ◆ Portais do SERPRO e aplicações em software livre;
- ◆ Programa de Software Livre do SERPRO – PSSL;



## Projetos em software livre

- ◆ Correio Livre (Expresso Livre);
- ◆ Chat (Mensagem Instantânea) – Jabber/PSI;
- ◆ VoIP;
- ◆ Segurança da intranet (IDS);
- ◆ Gerência de rede;
- ◆ **Rede Local Software Livre – RLSL.**



## O que é Rede Local Software Livre?

- ◆ Conjunto de sistema operacional mais programas que fornecem diversas funcionalidades de uma rede local;
- ◆ Ferramentas com licenças livres (GPL, BSD, etc);
- ◆ Alternativa a sistemas de rede local proprietários;
- ◆ Resultado do trabalho de múltiplos Centros de Especialização;



## Serviços

- ◆ Autenticação LDAP (Diretório Livre);
- ◆ Arquivamento remoto (SAMBA);
- ◆ Servidor de Impressão (CUPS);
- ◆ Transferência de arquivos (VsFTP);



## Serviços

- ◆ Resolução de nomes (DNS-Bind);
- ◆ Sincronismo de tempo (NTP);
- ◆ Configuração dinâmica do host (DHCP);
- ◆ Cache web (Squid);
- ◆ Serviço de backup (Bacula);



## Sistemas internos

- ◆ Saguí: instalação, atualização, correção e coleta;
- ◆ Babassu: Difusão de mensagens na rede local;
- ◆ SGB: Sistema de gestão de bilhetagem de impressão;
- ◆ IDS: segurança e monitoramento;
- ◆ Autenticação com certificado digital;
- ◆ Gerência da rede local (SIDE);



## Diretório

### ◆ Serviço de diretório LDAP;

- ◆ Catálogo de informações da RLSL;
- ◆ Base única de acesso comum aos serviços;
- ◆ Centralização da autenticação;

### ◆ Topologia:

- ◆ Multi-master;
- ◆ Replicação com slaves nas demais localidades;

### ◆ Softwares em uso:

- ◆ Ambiente misto de transição: RHDS com FDS/389;
- ◆ Plugins internos: fscota, smbpasswd e smbaddclass;
- ◆ Sistema interno de gestão operacional: SADIL.



## Arquivamento remoto

- ◆ **Armazenamento de arquivos no servidor RLSL:**
  - ◆ **Área pública (“global”):**
    - ◆ facilitar intercâmbio de conteúdos na empresa.
  - ◆ **Área setorial (“grupos”):**
    - ◆ centralização de arquivos relevantes a grupos de trabalho ou setores específicos.
  - ◆ **Área pessoal (“usuario”):**
    - ◆ Espaço para armazenamento de arquivos de trabalho com garantia de backup.
- ◆ **Acessíveis apenas após autenticação:**
  - ◆ Sistema integrado com diretório LDAP.



## Arquivamento remoto

### ◆ **Cliente RLSL:**

- ◆ Desenvolvido internamente;
- ◆ Versatilidade no acesso aos dados foi um requisito;
- ◆ Recupera e mapeia informações a partir do serviço de diretório;

### ◆ **Usuários em trânsito:**

- ◆ acessam seus dados da rede de origem;

### ◆ **Grupos interregionais:**

- ◆ Usuários de múltiplas localidades físicas compartilham dados em um determinado servidor.



## Arquivamento remoto

### ◆ Softwares em uso:

- ◆ Samba 3;
- ◆ Recursos do sistema operacional:
  - ◆ ACLs de sistema de arquivos (ext3);
  - ◆ Quota de disco;

### ◆ Samba:

- ◆ autenticação do acesso aos compartilhamentos;
- ◆ autenticação (logon) de estações Windows;
- ◆ Integração com domínios AD (relação de confiança);
- ◆ Integração com serviço de impressão Linux;



## Impressão

- ◆ **Serviço de impressão corporativa:**
  - ◆ Impressoras com interfaces de rede;
  - ◆ Requisitos como bilhetagem, quota e relatórios;
- ◆ **Topologia:**
  - ◆ Impressoras cadastradas e divulgadas pelo servidor;
  - ◆ Acesso direto às impressoras bloqueado;
- ◆ **Softwares em uso:**
  - ◆ CUPS como servidor de impressão;
  - ◆ Samba para integração CUPS - Windows;
  - ◆ Pykota, SNMP e PostgreSQL para bilhetagem;
  - ◆ Sistema interno de relatórios: SGB.



## Impressão

### ◆ **Pykota como sistema de bilhetagem:**

- ◆ Agente intermediário (backend) do CUPS;
- ◆ Consultas SNMPv3 ao contador físico das impressoras;
- ◆ Contagem interna caso SNMP não disponível;
- ◆ Armazenamento de dados em banco Postgresql;

### ◆ **Relatórios de impressão:**

- ◆ Necessidades especiais de uma empresa:
  - ◆ Extração de relatório para cobrança;
  - ◆ Discriminação de impressões e totalização por usuário, por grupo/setor e Unidade de Gestão;
- ◆ Ferramenta nativa ao Pykota não atende.



## Impressão

- ◆ **SGB: Sistema de Gerenciamento de Bilhetagem**
  - ◆ Sistema web desenvolvido internamente;
  - ◆ Objetivo: suprir os requisitos de relatórios avançados;
  - ◆ Ponte entre informações armazenadas pelo Pykota e dados dos usuários presentes no serviço de diretório;
  - ◆ Relatórios para usuários e gestores;
  - ◆ Envio de email com extrato mensal;
- ◆ **Opções de relatórios:**
  - ◆ Usuários: consulta de histórico de impressão mensal, saldo de quota e relatórios sumarizados ou detalhados;
  - ◆ Gestores: totais por impressora, por setor e por UG;



## Transferência de arquivos

### ◆ Alternativas para publicação de conteúdos:

- ◆ Objetivo original: disponibilizar a área pública via FTP;
- ◆ Usado como alternativa para situações em que e-mail ou o arquivamento remoto não atende;

### ◆ Topologia:

- ◆ Variável; soluções projetadas sob demanda:
  - ◆ Exemplo: solução para CECOM;
- ◆ Raiz FTP e WWW disponível aos administradores;

### ◆ Softwares em uso:

- ◆ VsFTP;
- ◆ Servidor web Apache;



## Transferência de arquivos

### ◆ **Estudo: solução para a área de comunicação**

#### ◆ Requisitos:

- ◆ Disponibilização de arquivos para acesso nacional;
- ◆ Acesso de leitura público, sem autenticação;
- ◆ Acesso de escrita apenas para CECOM;

### ◆ **Topologia:**

- ◆ Diretório de propriedade da CECOM no servidor;
- ◆ Acesso de escrita via Samba por meio de autenticação;
  - ◆ mapeamento automático, sem necessidade de ação nas estações dos usuários;
- ◆ Disponível na raiz FTP para acesso rápido e WWW para uso de recursos avançados (slideshow, thumbnail, etc).



## Sincronismo de tempo

### ◆ Elemento de infraestrutura chave:

- ◆ útil para usuários;
- ◆ essencial para diversos outros serviços de rede;

### ◆ Topologia:

- ◆ servidores base: [ntp.on.br](http://ntp.on.br) e [ntp2.on.br](http://ntp2.on.br);
  - ◆ servidor SERPRO/SUPCD: [websrve.base.serpro.gov.br](http://websrve.base.serpro.gov.br)
  - ◆ servidores RLSL;

### ◆ Softwares em uso:

- ◆ NTPv4 para Linux;



## Resolução de nomes

- ◆ **Elemento importante em redes locais:**
  - ◆ útil para administradores de redes;
  - ◆ essencial para navegação Internet dos usuários;
  - ◆ Implantação “homogeneizou” o serviço no SERPRO;
- ◆ **Topologia mista: finalidade dupla**
  - ◆ cache DNS para consultas de nomes Internet;
  - ◆ zonas de autoridade: hierarquia de nomes da Intranet;
  - ◆ redundância: pelo menos dois servidores por local;
- ◆ **Softwares em uso:**
  - ◆ Bind 9



## Resolução de nomes

### ◆ **Cache DNS:**

- ◆ Servidores cache disponíveis em cada regional ou escritório;
- ◆ Melhora no tempo de resposta a sítios Internet;

### ◆ **Topologia:**

- ◆ servidores SERPRO/SUPRE
  - ◆ Servidores corporativos SUPTI: ns1.serpro e ns2.serpro
    - ◆ servidores DNS por localidade + servidores RLSL



## Resolução de nomes

### ◆ Zonas de autoridade:

- ◆ Resolução de nomes: recurso indispensável para grandes Intranets;
- ◆ Hierarquização viabiliza delegação de subdomínios para cada localização;

### ◆ Topologia:

- ◆ servidores .serpro: ns1.serpro e ns2.serpro;
  - ◆ servidores regionais: rce.serpro, bsa.serpro, etc.



## Configuração dinâmica de rede em equipamentos

### ◆ **Protocolo DHCP**

- ◆ Atribuição dinâmica de parâmetros de rede de equipamentos;
- ◆ Essencial para a administração de redes locais;
- ◆ SERPRO: endereços IP atrelados a endereços MAC;

### ◆ **Topologia:**

- ◆ Servidor RLSL regional armazena as configurações necessárias daquela localidade;
- ◆ Não há integração entre servidores.

### ◆ **Softwares usados:**

- ◆ DHCPv3 para Linux;
- ◆ Webmin para gestão operacional.



## Cache web

- ◆ **Performance de navegação**
  - ◆ Economia de banda WAN;
  - ◆ Importante em localidades com links reduzidos;
    - ◆ Muito usado nos escritórios do SERPRO;
- ◆ **Topologia:**
  - ◆ Squid não hierárquico para cada localidade;
- ◆ **Softwares usados:**
  - ◆ Squid 2;



## Cache web

### ◆ **Estudo de caso: gateways do SERPRO**

- ◆ Gateways do SERPRO: conjunto de soluções proprietárias de filtro de conteúdo e cache web;
- ◆ Administração da SUPRE;

### ◆ **Estado atual:**

- ◆ Trabalho em conjunto SUPTI/SUPRE para implantação de Squid como cache web nos gateways;
- ◆ 3 máquinas com Squid + 1 máquina com a solução anterior hoje em produção;
- ◆ Estudo de substituição do filtro de conteúdos por soluções livres.



## Backup

### ◆ **Serviço indispensável para rede local**

- ◆ Importância dos dados de usuários no arquivamento remoto;
- ◆ Restauração do sistema com as configurações dos vários serviços (associações dhcp, zonas dns, etc);

### ◆ **Topologia:**

- ◆ Servidor RLSL com drive de fita;
- ◆ Backup de múltiplos servidores Linux e Windows via rede;

### ◆ **Softwares usados:**

- ◆ Bacula 2;
- ◆ Postgresql 8 para armazenamento dos catálogos;



## Backup

### ◆ Solução standalone

- ◆ Presente em todas as regionais do SERPRO (RLSL);
- ◆ Implantadi em clientes do SERPRO ;

### ◆ Recursos avançados:

- ◆ Suporte a tape library e multi-drive autochangers;
- ◆ Elementos de segurança: autenticação e criptografia na transmissão de dados;



## Babassu

### ◆ **Divulgação de mensagens**

- ◆ Sistema desenvolvido pelo CEUL;
- ◆ Necessidade suprir lacuna na divulgação de mensagens na rede local (“mensagens *pop-up*”);
  - ◆ Ex: indisponibilidade de servidores, manutenção de serviços, “incêndio”;
- ◆ Uso ampliado para atender às necessidades da Comunicação;

### ◆ **Topologia:**

- ◆ Servidor RLSL divulga para suas redes locais de seu escopo;
- ◆ Clientes Babassu em todas as estações Linux e Windows;



## Babassu

### ◆ Recursos

- ◆ Uso restrito a usuários pré-autorizados;
- ◆ Autenticação no serviço de diretório;
- ◆ Possibilidades de envio:
  - ◆ Toda a rede;
  - ◆ Usuários específicos;
  - ◆ Grupos de usuários agrupados por setor;



## Sagui

### ◆ Sistema de apoio à RLSL

- ◆ Sistema centralizado desenvolvido e administrado pelo CEUL;
- ◆ Viabilizou a implantação do GNU/Linux em dezenas de servidores e centenas de estações;

### ◆ Topologia:

- ◆ 4 módulos de funcionamento:
  - ◆ Instalação de servidores e estações;
  - ◆ Aplicação de correções (patches);
  - ◆ Controle de atualização;
  - ◆ Coleta de informações dos equipamentos;



## Sagui

### ◆ Instalação

- ◆ Arquivos de pré-configuração:
  - ◆ Red Hat / CentOS: kickstart (ks);
  - ◆ Debian / Ubuntu: preseed;
- ◆ Scripts de procedimentos:
  - ◆ Globais (todos os servidores)
  - ◆ Individuais por serviço (modularização da RLSL)

### ◆ Atualização

- ◆ Script de atualização do sistema operacional;
- ◆ Controle da execução (painel monitor);



## Sagui

### ◆ Correção

- ◆ Scripts de ajustes operacionais (patches);
- ◆ Controle de liberação
  - ◆ por perfil;
  - ◆ Por localidade;
- ◆ Histórico de lançamento de patches: informações do responsável e histórico de versões;
- ◆ Controle de execução;

### ◆ Coleta

- ◆ Scripts de coleta de informações sobre os equipamentos;



## Custo com licenciamento de software

### ◆ Anterior à RLSL + GNU/Linux:

- ◆ Licenças Windows para todas as estações;
- ◆ Licenças Novell Netware para servidores e custo adicional por elementos cadastrados no diretório (Edirectory);
- ◆ Estimativa de custo de licenciamento: **R\$1.500.000,00** (2007);

### ◆ RLSL v1

- ◆ Servidores RLSL Red Hat Enterprise 4;
- ◆ Serviço de diretório Red Hat Directory Service;
- ◆ Estimativa de custo com licenças para suporte: **R\$150.000,00**



## Custo com licenciamento de software

- ◆ **RLSL v2: software livre sem subscrição**
  - ◆ Servidores RLSL Debian Lenny (5);
  - ◆ Alternativa de SO: CentOS 5;
  - ◆ Serviço de diretório FDS/389;
  - ◆ Custo de licenciamento: **R\$ 0,00**;



## Perguntas?

paulo.arruda@serpro.gov.br - (81) 2126.4093

marcelo.rabelo-andrade@serpro.gov.br - (81) 2126-4109