BANCO POSTAL - Plataforma Tecnológica

1. Arquitetura da Aplicação

1.1. O Banco Postal utiliza uma arquitetura cliente/servidor WEB em "n" camadas:

1.1.1. **Camada de Apresentação** – estações de atendimento, nas agências da ECT;

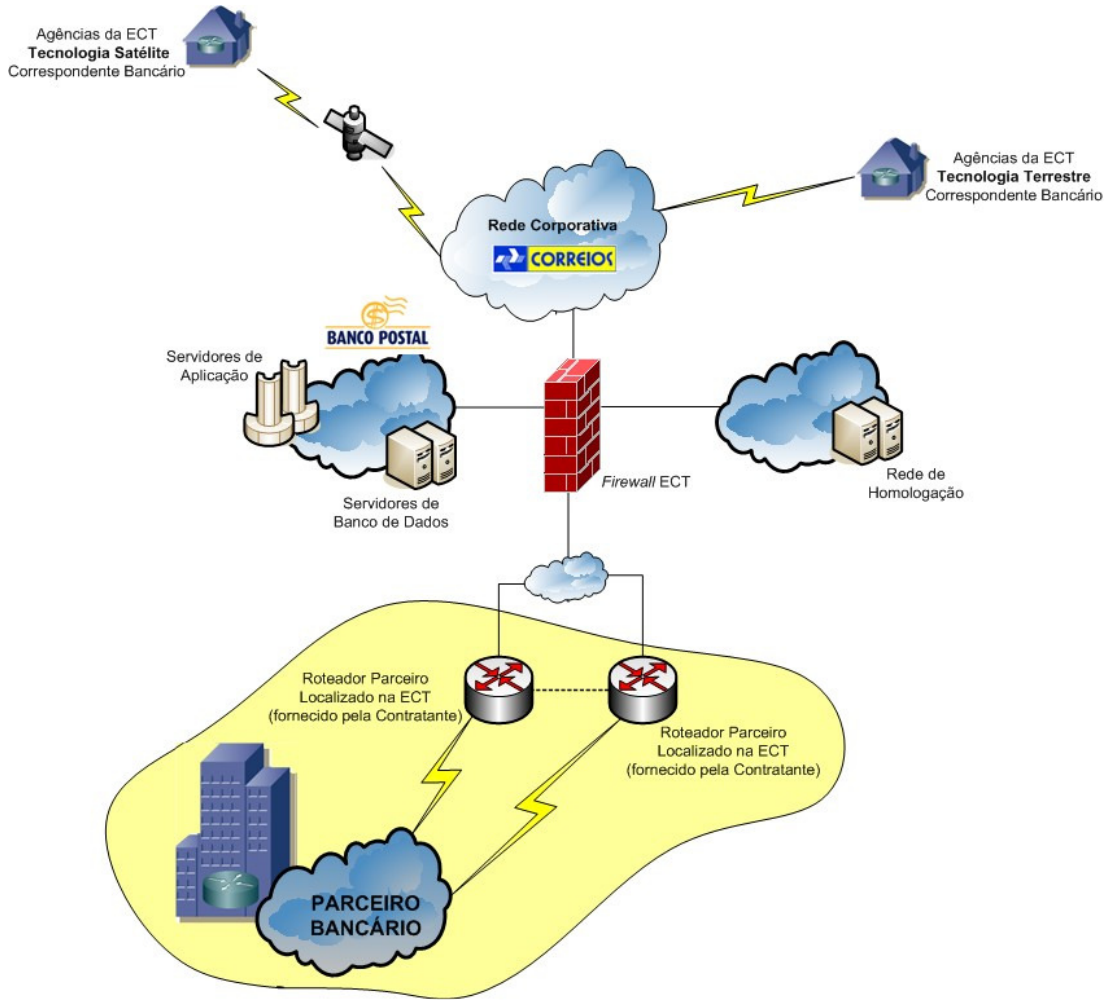
1.1.2. **Camada de Conversão de formato de mensagens** – cluster servidor de aplicação, centralizado em Brasília-DF;

1.1.3. **Camada de Regras de Negócio** – cluster servidor de aplicação, centralizado em Brasília-DF;

1.1.4. **Camada de Persistência** – cluster servidor de Banco de Dados, centralizado em Brasília-DF;

1.1.5. **Camada de Armazenamento** – área de armazenamento, centralizada em Brasília-DF.

1.2. Desenho esquemático da solução



1.3. Site de Atendimento

1.3.1. O Site de Atendimento compreende as Agências da ECT, para atendimento aos clientes, onde são executadas as transações financeiras. É composto de microcomputadores e periféricos para operacionalização dos pontos de atendimento e retaguarda;

1.3.2. Os microcomputadores utilizados para executar as transações financeiras dentro do conceito de Banco Postal são os mesmos que executam o SARA – Sistema de Automação da Rede de Atendimento postal da ECT. Os dois sistemas, Banco Postal e SARA, são integrados por meio de uma rotina (camada) de integração. Os periféricos (PIN-pad, impressora de comprovante, leitor de cartão magnético, leitor de código de barras, CMC7 e impressora jato de tinta) são compartilhados pelos dois sistemas. É requisito imprescindível para a operação do sistema Banco Postal que o SARA esteja instalado e operacional no mesmo ponto de atendimento ou retaguarda;

1.3.3. A estação de atendimento utiliza, atualmente, o Sistema Operacional Windows XP SP3 ou Windows 2000 com os patches e atualizações devidamente aplicados. Requisitos para o SARA e Banco Postal: Internet Explorer 6 SP2; Java (JRE - *Java Runtime Environment*) na versão 1.5.05. Versões posteriores do Windows, do Java e do Internet Explorer, bem como sistemas operacionais de código aberto (LINUX) poderão ser utilizados futuramente desde que homologados pela ECT para operacionalização com os sistemas SARA e Banco Postal;

1.3.4. O site de atendimento está conectado ao Site Autorizador por meio da Rede Corporativa da ECT.

1.4. Site Autorizador da ECT

1.4.1. O Site Autorizador é o responsável pelas autorizações das transações internas da ECT e roteamentos das transações financeiras realizadas com o Banco Parceiro, bem como gerenciar e armazenar dados do Banco Postal;

1.4.2. O Centro Corporativo de Dados da Administração Central – CCD/AC, em Brasília-DF, sendo o ambiente de produção composto por quatro clusters de servidores RISC, um para HTTP, um para IST, um para a camada de aplicação e outro para a de banco de dados do sistema Banco Postal;

1.4.3. Os servidores de aplicação e de banco de dados, o *storage* corporativo e a infraestrutura de comunicação entre o Site Autorizador da ECT e as Unidades de Atendimento, são disponibilizados pela ECT e de uso exclusivo da ECT;

1.4.4. Os *clusters* de servidores de aplicação e de banco de dados do sistema Banco Postal estão conectados a uma rede SAN (*Storage Area Network*), LAN (*Local Area Network*) e à rede WAN (*Wide Area Network*) da ECT;

1.4.5. Os *clusters* de banco de dados gerenciam a base de dados armazenada no *storage* corporativo, processando em ambiente RISC com SGBD Oracle;

1.4.6. Os *clusters* de aplicação executam os processos de forma balanceada, garantindo que a paralisação de um equipamento não acarrete na indisponibilidade do serviço;

1.4.7. Todas as operações bancárias intermediadas pelas agências da ECT, como Correspondente Bancário, serão registradas em bases de dados, tanto pelo Banco Parceiro quanto pela ECT.

1.5. Sala de Monitoração.

1.5.1. A Sala monitora a infraestrutura de rede e de produção da ECT, de forma centralizada, atuando como suporte de 1º nível no tratamento de incidentes, por meio de ferramentas de gerência de propriedade da ECT.

2. Características da Solução

2.1. Para cada transação está definido um fluxo e um leiaute específico;

2.2. Todas as transações, nas estações de atendimento, são executadas em tempo real. O sistema não possui tratamento para processamento (*off-line*) de transações em caso de inoperância dos servidores do parceiro, da ECT, da rede de comunicações e Estações de Trabalho;

2.3. Existe tratamento de conciliação com o parceiro de negócio, realizado diariamente no turno da madrugada, para os dados do movimento diário;

2.4. As agências da ECT (e outros canais de atendimento providos pela Empresa) podem operar com estação de atendimento, sendo os aplicativos locais dimensionados de forma a prever o compartilhamento de todos os recursos com todos os demais sistemas no *front-office*;

2.5. A solução integra o caixa de atendimento bancário com o caixa das operações postais num único caixa;

2.5.1. O fechamento da agência (atividade bancária e postal), para todos os caixas, é efetuado pelo gerenciador de caixa, a partir das informações fornecidas pelo módulo de automação bancária;

2.6. Todas as transações financeiras geradas nas unidades de atendimento da ECT assim como seu retorno por parte do Banco Parceiro utilizam o padrão ISO-8583/ECT.

3. Arquitetura de Comunicação

3.1. O protocolo padrão de rede utilizado pela ECT é o TCP/IP (*Transmission Control Protocol/Internet Protocol*);

3.2. No âmbito da ECT, todos os dados trafegados entre a ECT e o Banco Parceiro serão monitorados e protegidos por equipamentos de segurança da ECT.

3.2.1. O Banco Parceiro deverá fornecer, no mínimo, 2 (dois) enlaces principais dedicados de comunicação (sendo, respectivamente, 1 para produção e outro para homologação) e 2 (dois) enlaces de contingência dedicados de comunicação (sendo, respectivamente, 1 para produção e outro para

homologação).

3.2.2. O enlace de contingência deve ser disponibilizado por operadora de telecomunicação distinta do principal;

3.2.3. Cada enlace deve possuir roteadores próprios e exclusivos, tanto no Banco Parceiro quanto na ECT;

3.2.4. Na ocorrência de falha ou intermitência do enlace principal, a contingência deve ser acionada automaticamente, no prazo máximo de 5 (cinco) segundos a partir da ocorrência da falha ou intermitência;

3.2.5. Para efeito de dimensionamento dos enlaces entre o Banco Parceiro e a ECT, a taxa média de utilização a cada 10 (dez) minutos para enlaces terrestres e a cada 15 minutos para enlaces satélites (se for o caso), deve ser inferior a 60% (sessenta por cento) da velocidade nominal para cada enlace;

3.2.6. Os dois enlaces deverão ter capacidades idênticas, de forma que em caso de falha do enlace principal todo o tráfego seja cursado pelo enlace de contingência sem perda de qualidade, observando os preceitos supra associados ao prazo de acionamento e à taxa média de utilização.

3.3. O Banco Parceiro deve prover uma rede logicamente independente e isolada de qualquer outra rede, inclusive da Internet. O isolamento deverá ser realizado no nível da camada de enlace do protocolo TCP/IP;

3.4. O Banco Parceiro deve aplicar implementações de segurança de acesso nos roteadores sob sua administração, tais como: autenticação de roteador CPE (C*ustomer-Provided Equipment*), autenticação centralizada de usuários com privilégio de visualização; controle de acesso aos dispositivos através de filtros de pacotes e de listas de acesso de forma a garantir os níveis de segurança adequados aos dispositivos;

3.5. Caberá ao Banco Parceiro proceder a ativação elétrica dos equipamentos, além de suas conexões lógicas à Rede Corporativa da ECT, seguindo os padrões definidos pela ECT;

3.6. O protocolo da rede WAN (*Wide Area Network*) do Banco Parceiro deve ser TCP/IP, devendo as transferências de dados para os serviços contratados estarem calcadas nesse protocolo;

3.7. Cabe ao Banco Parceiro obediência às normas, à política de segurança e aos padrões técnicos da ECT;

3.8. Os enlaces de comunicação WAN que interliga o Banco Parceiro e a Rede Corporativa da ECT devem atender aos seguintes indicadores de níveis de serviço:

3.8.1. Disponibilidade mensal: 99,9% (noventa e nove vírgula nove por cento);

3.8.2. Latência máxima: 50 (cinqüenta) milissegundos;

3.8.3. Tempo de reparo máximo: 1 (uma) hora para os enlaces de produção (principal e contingência) e 3 (três) horas para os enlaces de homologação (principal e contingência);

3.9. É de responsabilidade do Banco Parceiro o dimensionamento do porte, a instalação, a configuração, a operação, a manutenção, o monitoramento e a gerência dos roteadores e dos enlaces necessários ao funcionamento da rede que interliga o Banco Parceiro e a ECT, em ambos os lados.

3.10. As manutenções, preventiva e corretiva, e a atualização da infraestrutura da rede que interliga o Banco Parceiro e a ECT, bem como o suporte técnico, deverão ser de responsabilidade e expensas do Banco Parceiro, que deverá informar os números telefônicos para contato em casos de incidentes nesse ambiente;

3.11. O Banco Parceiro deverá comunicar a ECT, com antecedência mínima de 48 (quarenta e oito) horas, quando for necessário agendar manutenções preventivas no ambiente;

3.12. É obrigação do Banco Parceiro prestar sempre todos os esclarecimentos técnicos à equipe da ECT em caso de incidente ou quando demandada, imediatamente a sua ocorrência;

3.13. É obrigação do Banco Parceiro monitorar e gerenciar continuamente seus elementos de forma pró-ativa e manter a ECT informada;

3.14. O Banco Parceiro deverá fornecer um portal ou ferramenta de gerência, pelo próprio enlace, ou alternativamente pela WEB, que permita a ECT visualizar disponibilidade, volume de tráfego, desempenho de CPU, memória e tempo de resposta dos enlaces e roteadores da solução e relatórios mensais contendo no mínimo visualização *on-line*.

4. Segurança da informação

4.1. As informações devem receber classificação conforme norma ABNT NBR ISO/IEC 27002 (confidencial, restrita, interna ou pública), pelo Banco Parceiro, indicando as ameaças e as vulnerabilidades a que estão sujeitas, o impacto decorrente da concretização de incidentes e a importância dessas informações para o negócio. O tratamento dessas informações devem obedecer a essa classificação;

4.2. Os recursos que armazenam, processam ou transportam informação ou dados, merecem o mesmo tratamento que é dado à própria informação ou dados e só devem ser utilizados para os fins estabelecidos e de acordo com as Normas de Segurança da Informação da ECT;

4.3. O Banco Parceiro e os prestadores de serviços terceirizados devem estar em conformidade com a Política de Segurança da ECT e com as normas ABNT NBR ISO/IEC 27001 e 27002;

4.4. O Banco Parceiro deve prover a segurança de seus equipamentos, envolvidos na solução do Banco Postal de forma a garantir restrição de acesso a pessoas não autorizadas, de acordo com a classificação da informação processada;

4.5. Quando da necessidade de acesso do Banco Parceiro no ambiente de homologação da ECT, deverá haver o controle de acesso aos serviços e às aplicações, sendo obrigatório, no mínimo, o uso de ID único e senha do usuário;

4.6. A implementação de novas aplicações e as principais manutenções nos softwares e aplicações existentes devem seguir um processo de documentação, especificação, teste, controle de qualidade e gerenciamento de implementação;

4.7. O Banco Parceiro deve manter o controle de versão para todos os softwares e atualização de aplicações;

4.8. O Banco Parceiro deve assegurar que as implementações de mudanças sejam realizadas tempestivamente e no local adequado, sem prejudicar os processos envolvidos;

4.9. A ECT utiliza o padrão 3DES (*Triple Data Encryption Standard*) para criptografia das senhas dos clientes (PIN – *Personal Identification Number*) do Banco Postal;

4.10. O Banco Parceiro deverá fornecer as chaves-mestre (*Master-Keys*) de criptografia;

4.11. As transações eletrônicas do Banco Postal devem estar em conformidade com a norma ISO 8583/ECT;

4.12. A solução contém mecanismos de segurança que garantem a efetiva conclusão de todos os serviços e transações registrados, estando previstos cancelamentos ou recuperações automáticas no caso de desistências, falhas, queda de comunicação, queda de energia, ou ocorrências afins;

4.13. O Banco Parceiro deverá garantir a existência de trilhas de auditoria de todas as transações efetuadas por qualquer dos aplicativos que a compõem, permitindo a identificação de autoria e responsabilidade de todos os indivíduos associados com a transação, Data e Hora (HH:MM:SS).

****