



Diagnóstico de Infraestrutura
Programa de Reestruturação Organizacional
Elaboração e Implantação do Portal de Governança de TI da
TERRACAP
FASE I

ANEXO IV

SUMÁRIO

| | |
|---|----|
| 1. Introdução | 3 |
| 2. Considerações | 3 |
| 3. Conceituação | 3 |
| 4. Análise | 4 |
| 4.1 Parque de Equipamentos..... | 4 |
| 4.2 Softwares e Frameworks..... | 7 |
| 4.3 Banco de Dados e Aplicações | 10 |
| 4.4 Sistemas Operacionais de Banco de Dados e Aplicações..... | 12 |
| 5. Topologia de Rede..... | 12 |
| 5.1 Administração de Usuários | 14 |
| 5.2 Conexão entre Hosts..... | 14 |
| 5.3 Topologia Firewall | 16 |
| 6. Teste de Intrusão e Vulnerabilidade..... | 17 |
| 6.1 Teste Ambiente Físico..... | 17 |
| 6.2 Teste Ambiente Lógico..... | 18 |
| 7. Considerações | 19 |
| 8. Execução e Aprovação | 20 |

1. Introdução

Apresentar-se-ão os resultados obtidos no levantamento e análise da gestão dos recursos de Infraestrutura de TI da TERRACAP, que contemplam hardware, software e outros dispositivos sob a responsabilidade da DISUP – Divisão de Suporte da CODIN.

Os dados reunidos neste documento serão utilizados como insumo para a elaboração do relatório do Plano Diretor de Tecnologia da Informação – PDTI.

2. Considerações

As informações que embasaram este diagnóstico foram extraídas de documentos fornecidos pela CODIN/TERRACAP, entrevistas com aplicação de questionários, além de visita monitorada aos ambientes e instalações de infraestrutura de TI da TERRACAP.

3. Conceituação

Visando a atender ao Plano Diretor de Tecnologia da Informação da TERRACAP, consideram-se:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade:** assegurar a exatidão da informação desde a sua criação.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Criticidade:** grau de importância da informação para a continuidade dos negócios da TERRACAP.
- **Segurança da Informação:** preservação da confidencialidade, integridade e disponibilidade da informação. Também, outras propriedades podem estar envolvidas, tais como, autenticidade, responsabilidade, não repúdio e confiabilidade.
- **Ativo:** qualquer coisa que tenha valor para a empresa.
- **Recurso:** além da própria informação eletrônica, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento.
- **Usuário:** quem utiliza, de forma autorizada, informações da TERRACAP.

- Avaliação de risco: avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência.
- Incidentes de Segurança: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- Gerenciamento de Risco: processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação a um custo aceitável.

4. Análise

Considerando que a atividade fim da CODIN é:

- Disponibilizar o ambiente tecnológico adequado para os negócios da TERRACAP por meio de:
 - ✓ Serviços de desenvolvimento e manutenção de sistemas;
 - ✓ Gestão de banco de dados;
 - ✓ Serviço de suporte e atendimento ao usuário;
 - ✓ Serviço de segurança da informação e
 - ✓ Serviço de rede de comunicação e demais serviços afins.

Para o desenvolvimento do PDTI, faz-se necessário o levantamento atual dos recursos de TI, no intuito de verificar se esses são adequados e permitem a execução de forma satisfatória dos processos definidos.

Desta forma, relacionamos abaixo a infraestrutura levantada no período de 05/03/2012 a 27/04/2012, não levando em consideração quaisquer aumentos ou reduções do parque da TERRACAP, fora deste período, ou que não tenham sido comunicadas antes da validação do documento.

4.1 Parque de Equipamentos

O quadro a seguir apresenta os ativos: de servidores, *appliances*, *storages*, bibliotecas robotizadas, *switches*, *access points*, roteadores e outros *hardwares* diretamente ligados à infraestrutura de TI necessários a operacionalização das atividades da CODIN.

| Ativos | Marca / Modelo | Descrição | Quantidade |
|-----------------------------|--------------------------------------|---|------------|
| Servidores Blade | Blade HP ProLiant | Blade HP ProLiant BL460c G6 Server com 2 proces. Quad Intel(R) Xeon(R) CPU E5540 @ 2.53GHz 32Gb memórias. | 9 |
| | | Blade HP ProLiant BL460c G6 Server com 2 proces. Quad Intel(R) Xeon(R) CPU E5540 @ 2.53GHz 16Gb memórias. | 6 |
| Servidores Racks | HP ProLiant DL180 G6 Server | Processadores 2 Quad-Core Intel Xeon E5606 - 2.13 GHz, 18 GB memórias. | 1 |
| Appliances Hardware | Firewall Check Point | Firewall Check Point UTM 2270 | 2 |
| | Gerencia Check Point | Gerencia Check Point Smat -1 5 | 1 |
| | Filtro Web Optenet b200 | Optenet b200 | 1 |
| Storages | NetApp FAS3140 | NetApp DS14MK2 com 160T | 1 |
| | NetApp DS14MK2 | | 15 |
| Bibliotecas Robotizadas | HP StorageWorks MSL8096 Tape Library | Tape Library HP MSL8048, dois drives LTO4, FC, 48 fitas 1.6TB | 1 |
| Switches Fibre Channel (FC) | Brocade Turbolron | 4 Portas 10/100/1000 RJ45 + 24 10 GbE/1 GbE dual-speed ports | 2 |
| Switches de Core | 3Com 8810 | 24-Port 1000Base-X (SFP) IPv6 Module Fibre | 1 |
| | | 360 GBPS ETHERNET FAST ETHERNET FABRIC MODULE | 1 |
| | | 48-Port Gigabit Switching Module | 1 |
| | | 2000 Watt AC Power Supply | 2 |
| Switches de Acesso | 3Com 5500G-EI | Switch 5500-EI - 24x 10/100 Mbps + 4x mini-GBIC | 42 |

| Ativos | Marca / Modelo | Descrição | Quantidade |
|-------------------------------------|--------------------------------------|---|------------|
| | 3Com Switch 4200G | Switch 4200G - 20x 10/100/1000Mbps + 4x mini-Gbic ou 4x 10/100/1000 (Combo) + 1x Slot 10Giga XENPAK | 4 |
| Switch Central Rede Wireless | H3C WX3024 | H3C WX3024 24 × 10-/100-/1000-Mbps electrical ports | 1 |
| Distribuidor de Fibras | Distribuidor Interno de Fibras | Genérico | 7 |
| Access Points (APs) | H3C WA2600 Series WLAN Access Points | 2.4 GHz or 5 GHz frequency of the WLAN and supports the four modes of IEEE802.11a, IEEE802.11b, IEEE802.11g, and IEEE802.11n. | 9 |
| | D-LINK / DIR-615 | Compatível com 802.11B (11 Mbps) / 802.11G (54 Mbps) / 802.11N (300 Mbps). Possui 04 portas LAN 10/100 Mbps fast ethernet MDI/MDIX e 01 porta WAN 10/100 Mbps fast ethernet MDI/MDIX. | 1 |
| Circuito CFTV | Intelbras VD 16E 480 (DVR) | VD 16E 480 - Gravador digital de vídeo (DVR) | 1 |
| | INTELBRAS - VP 480 S | CCD Sony 1/3" super had 480 linhas de resolução horizontal Função Day & Night Tensão de alimentação 12 Vdc ou 24 Vac (automática) | 5 |
| Roteadores Internet | Cisco 2851 router | 2851 w/ AC PWR, 2GE, 4HWIC, 3PVDM, 1NME-XD, 2AIM, IP BASE, 128F/512D | 2 |

| Ativos | Marca / Modelo | Descrição | Quantidade |
|---------------------------------------|------------------------------------|--|------------|
| | Tellabs 6325 Edge Node Multiplexer | Multi-Service Provisioning Platform (MSPP) 1U height 44 mm SDH, PDH and Data services 2.5 Gbps SDH, PDH, Colored WDM and IP Ethernet switching (VLAN, MAC & MPLS) | 1 |
| Roteadores LP | Cisco 1800 Series Router | Cisco 1841 Modular Router w/2xFE, 2 WAN slots, 64 FL/256 DR | 1 |
| Refrigeração | Eletrolux CFI36 | Ar Condicionado Split Teto versão 36 mil BTUs Frio | 2 |
| | Carrier Space 42XQC036515LC | Ar Condicionado Split Teto 36000 BTU/s Frio | 1 |
| Cofres para Cópia de Segurança | LAMPERTZ / 60 DIS S-100 | P/Armazenamento de Fitas DAT CPD 509 (240 Kg) | 1 |
| | LAMPERTZ / 120 DIS S-13 | P/Armazenamento de Fitas DLT CPD 507 (445 Kg) | 1 |
| | LAMPERTZ / 120 DIS S-15 | P/Armazenamento de Fitas LTO-2 e LTO-3 Depósito (922 Kg) | 1 |

4.2 Softwares e Frameworks

O quadro a seguir apresenta os sistemas operacionais, aplicativos, *softwares* de gerência, *SGBDs*, servidores de aplicação, servidores *Web*, ferramentas e *frameworks* de desenvolvimento em uso na CODIN.

| Software | Nome / Versão | Descrição |
|---------------------------------------|---|---|
| Sistema Operacional | MS/Windows 2003 Server Pro | Sistema Operacional de 32 bits. |
| | MS/Windows 2008R2 Server Enterprise | Sistema Operacional de 64 bits. |
| | MS/Windows XP Prof. (Port) | Sistema Operacional de 62 bits. |
| | MS/Windows Vista Buss (Port) | Sistema Operacional de 32 bits. |
| | MS/Windows 7 Pro (Port) | Sistema Operacional de 64 bits. |
| | Linux Ubuntu Server 10.10 2.6.35x86_64 GNU/Linux | Sistema Operacional de 32 bits. |
| Servidores Web | Apache 2 | Sistemas corporativos PHP. |
| | Tomcat6 | Sistemas corporativos JAVA. |
| | IIS | Sistemas corporativos ASP.NET. |
| Servidores de Aplicação | Windows Server 2008R2 Enterprise | Sistemas corporativos forms oracle. |
| Aplicativos de Desenvolvimento | MS/Office Professional Plus 2010 64Bit | Suíte de Aplicativos para Escritório. |
| | MS/Office Professional Plus 2010 32Bit | Suíte de Aplicativos para Escritório. |
| | MS/Office Professional Plus 2003 32Bit | Suíte de Aplicativos para Escritório. |
| | MS/Office Professional Plus 2003 64Bit | Suíte de Aplicativos para Escritório. |
| | Dicionário Houais WEB | Dicionário de língua portuguesa. |
| | MS / Visio 2010 32Bit (StandardProfessionalPremium) | Software de Modelagem de Programas e Bancos de Dados. |
| | MS / Project Professional 2010 32Bit | Software de Gestão/Gerência de Projetos. |

| Software | Nome / Versão | Descrição |
|----------|------------------------------------|---|
| | MS/Project Professional 2010 64Bit | Software de Gestão/Gerência de Projetos. |
| | MS/Exchange 2010 Enterprise | Software de Servidor de Mensagens e Colaboração. |
| | AutoCAD Versão 2010 | É utilizado principalmente para a elaboração de peças de desenho técnico. |
| | AutoCAD Versão 2010 | É utilizado principalmente para a elaboração de peças de desenho técnico. |
| | CorelDRAW Graphics Suite 12 | Software Gráfico (Desenho Vetorial). |
| | McAfee e Policy Orchestrator 4.6 | Software Antivírus e AntiSpam para estações de trabalho e servidores. |
| | Optenet Security Suite | Software Filtro de conteúdo Web. |
| | OCOMON 1.40 | Software abertura de chamando. |
| | McAfee E-mail and Web Security 5.1 | Software de Antispam de E-mail. |
| | Google Enterprise Server | Software para geoprocessamento. |
| | Sharepoint Microsoft 2010 | Software para Gerenciar documentos e publicar relatórios. |
| | CommVault Simpana 9 | Software para Gerenciamento de Backup. |
| | Windows Server Update Service 3.0 | Gerenciar a distribuição de atualizações que são lançadas pelo serviço Microsoft Update. |
| | Active Directory 2008R2 | Mantêm dados como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. |
| | Check Point Firewall R75.20 | Software de Segurança de acesso interno e externo. |
| | SmartDashboard R75.20 | Software de Gerenciamento do firewall, Check Point. |

| Software | Nome / Versão | Descrição |
|----------|--------------------------------------|---|
| | Nagios® Core™ 3.2.3 | Software de Monitoramento de Servidores e Serviços. |
| | OCS Inventory NG 2.0.2 | Software de Inventário de Hardware e Softwares. |
| | GLPI | Software para Gerenciar a abertura e fechamento de chamado. |
| | Exchange Management Console | Software de Gerencia de correio eletrônico Exchange 2010. |
| | Open Fire | Software de Chat Corporativo. |
| | VMware 5.0 ESXi | Software de Virtualização de Sistemas Operacionais. |
| | iMC PLAT 5.0 SP1 | Software de Análise de Rede para Servidores HP. |
| | VMware vSphere Client | Software de Gerencia de máquinas virtuais vmware. |
| | HP BladeSystem Onboard Administrator | Software de Gerencia de Servidores Blade HP. |
| | H3C Series Wireless LAN Device | Software de Gerencia de Access Point 3Com. |
| | Embratel.net.br | Software de Monitoramento de Tráfego Circuito internet. |
| | PHPMYADMIN 2.11.0 | Ferramenta de Administração de My SQL. |

4.3 Banco de Dados e Aplicações

O quadro a seguir mostra os bancos de dados, seus versionamentos e aplicações *Oracle* disponíveis e administradas pela equipe de TI da CODIN.

| Produto | Versão | Comentário |
|--|-------------------|---|
| Oracle Database Enterprise Edition | 10gR2 | Software de Gerenciamento de Banco de Dados. |
| Real Application Cluster | 11gR2 | Clusterização de banco de dados Oracle. |
| Partitioning | 10gR2 | Pacote de implementação de particionamento de tabelas banco de dados. |
| Oracle Database Vault | 10gR2 | Pacote de implementação de segurança em banco de dados. |
| Oracle Spatial | 10gR2 | Banco de dados Geo-referencial e Geo-espacial. |
| Diagnostics Pack | 10gR2 | Pacote de diagnósticos em banco de dados. |
| Tuning Pack | 10gR2 | Pacote de implementação de melhorias em banco de dados. |
| WebLogic Server | 10.3.2.0 | Servidor de Aplicação Java, Webservice, Integração de aplicações, servidor de aplicação forms e reports. |
| Oracle Fusion Middleware | 11gR2 | Integração entre aplicações corporativas (gerenciamento e segurança de webservices, regras de negócio, eventos, monitoração das atividades de negócio). |
| Oracle Grid Control | 11gR2 | Monitoramento de aplicações, banco de dados e servidores voltada para soluções Oracle. |
| Oracle Business Intelligence Suite Enterprise Edition Plus – Processor Perpetual | 11gR2 | Data Warehouse e Business Intelligence – aplicação gerencial para auxílio, prospecção e tomada de decisão baseado em fatos históricos. |
| Oracle Business Process Management Suite | 11g | Gerenciamento de Processos de negócio da TERRACAP. |
| Oracle SOA Suite | 11g | Arquitetura Orientada a serviços. |
| SQLServer 2005 | 2005 | Sistema Gerenciador de Banco de dados. |
| SQLServer 2008 R2 | 2008 R2 | Sistema Gerenciador de Banco de dados. |
| SVN | 1.6.6 (r40053) | (Sistemas de controle de Versão) |

| Produto | Versão | Comentário |
|------------|----------|--|
| PostgreSQL | 8.4 | Sistema Gerenciador de Banco de dados. |
| MySQL | 5.0.67-0 | Sistema Gerenciador de Banco de dados. |

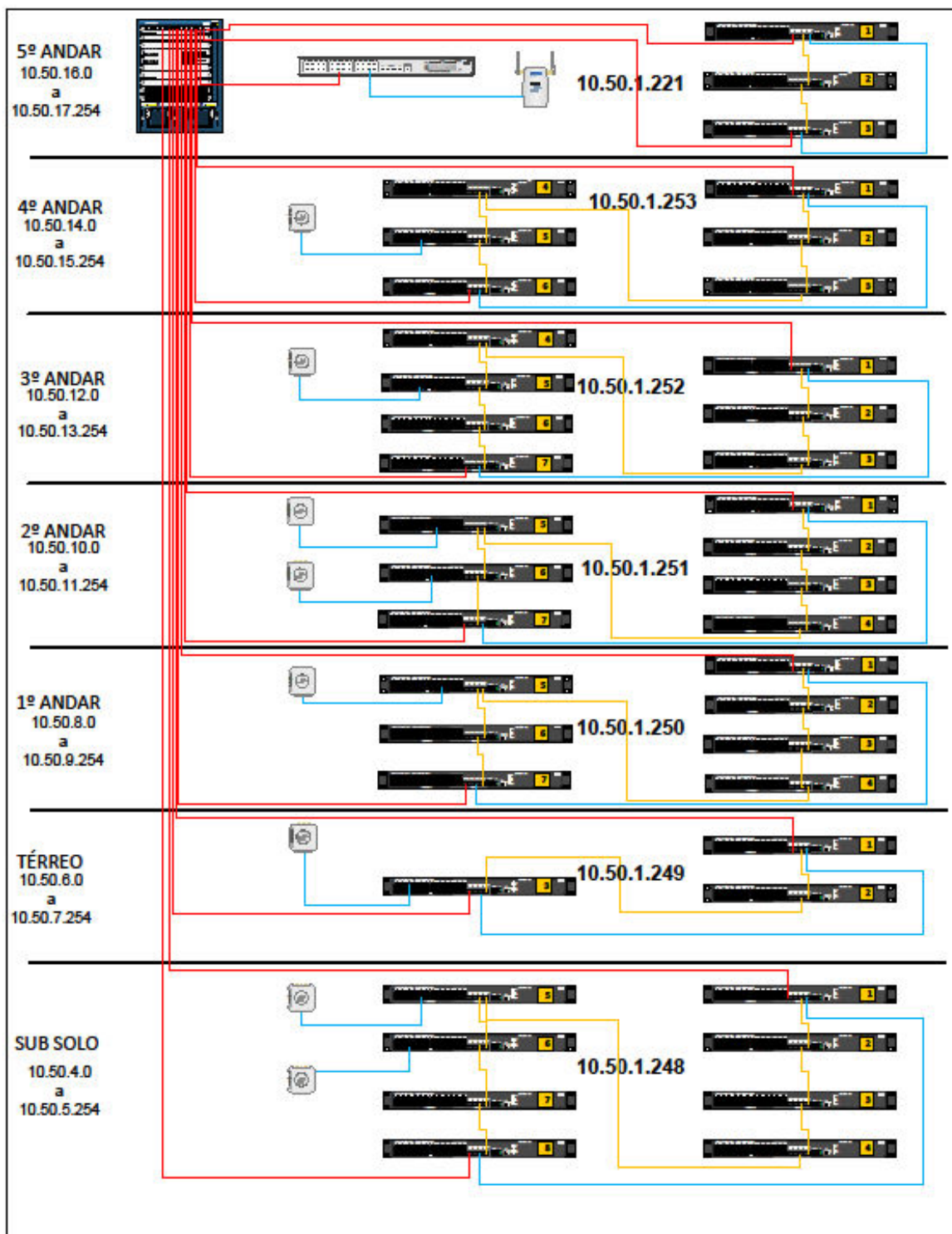
4.4 Sistemas Operacionais de Banco de Dados e Aplicações

O quadro a seguir apresenta os sistemas operacionais, utilizados nos servidores de bancos de dados e aplicações *Oracle*, disponíveis e administradas pela equipe de TI da CODIN.

| Produto | Versão | Comentário |
|---|---------|--|
| CentOS release 5.6 (Final) 2.6.18 238.12.1.el5 | 5.6 | Sistema operacional Linux 64 bits. |
| Red Hat Enterprise Linux Server release 5.6 (Tikanga) 2.6.18 238.12.1.el5 | 5.6 | Sistema operacional Linux 64 bits. |
| Red Hat Enterprise Linux Server release 5.6 (Tikanga) 2.6.18 238.19.1.el5 | 5.6 | Sistema operacional Linux 64 bits. |
| Red Hat Enterprise Linux Server release 5.7 (Tikanga) 2.6.18 274.el5xen | 5.7 | Sistema operacional Linux 64 bits. |
| Windows Server 2008 R2 Enterprise 64bits | 2008 | Sistema operacional Microsoft 64 bits. |
| Ubuntu 10.04.2 64bits | 10.04.2 | Sistema operacional Linux 64 bits. |

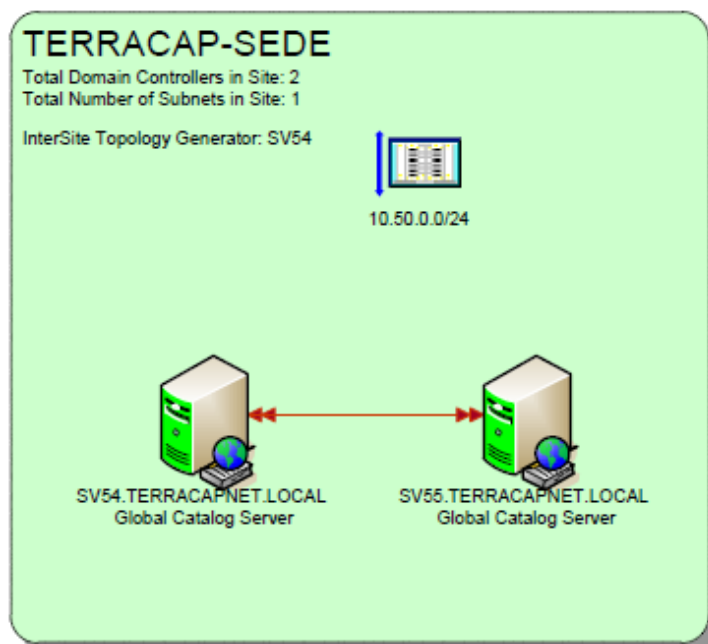
5. Topologia de Rede

O diagrama abaixo representa a forma como está estruturado o tráfego de informações através dos dispositivos conectados a rede.



5.1 Administração de Usuários

O quadro abaixo é uma representação dos dois *DS's* (*Domain Server*) da rede TERRACAP responsáveis pelo armazenamento e gerenciamento dos recursos de rede e de usuários – *AD* (*Active Directory*).



5.2 Conexão entre Hosts

O quadro abaixo representa logicamente a ligação e o tráfego de informações entre os hosts da rede TERRACAP, bem como o número de portas abertas em cada um dos *Hosts* nas datas do levantamento.

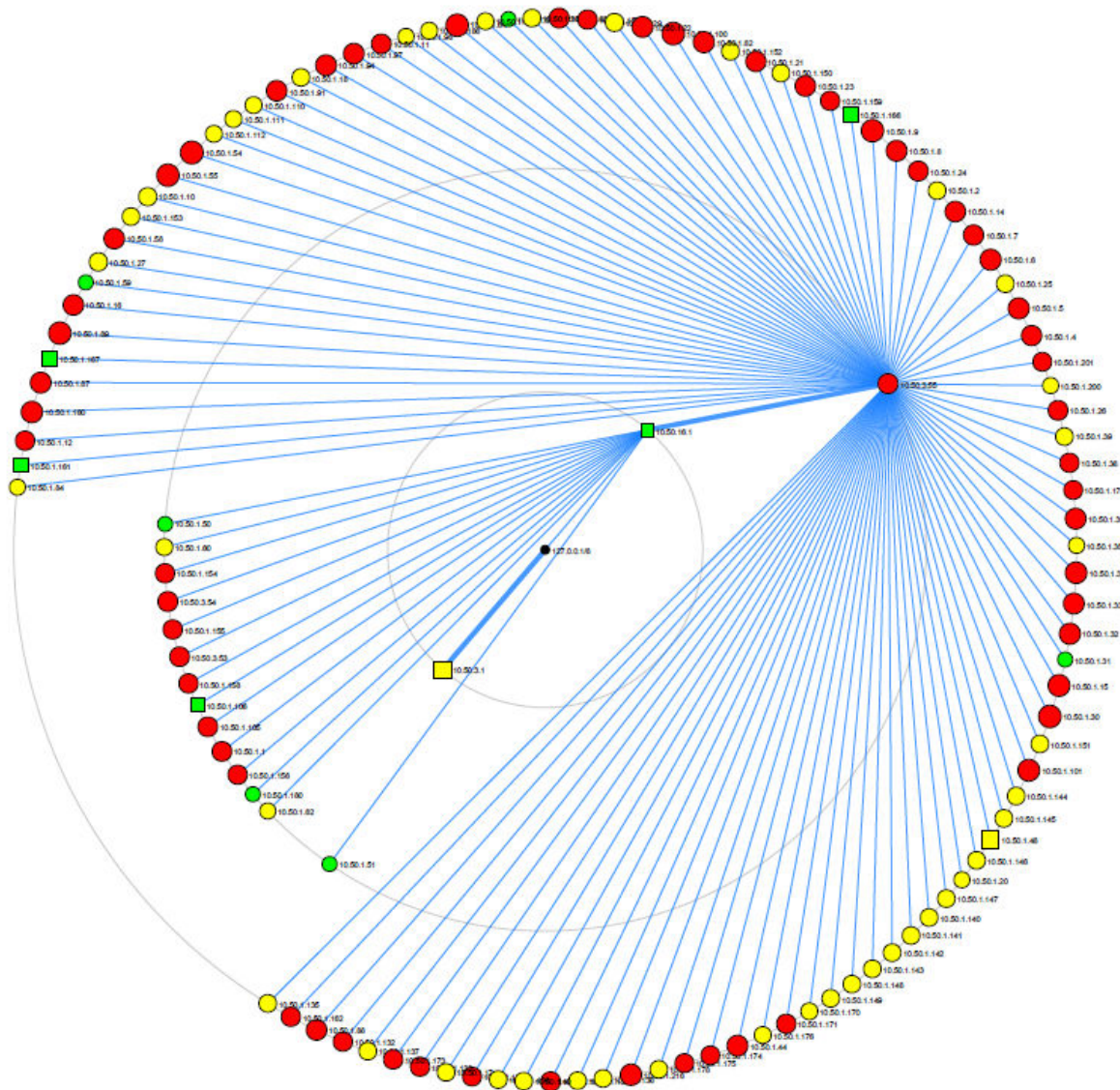









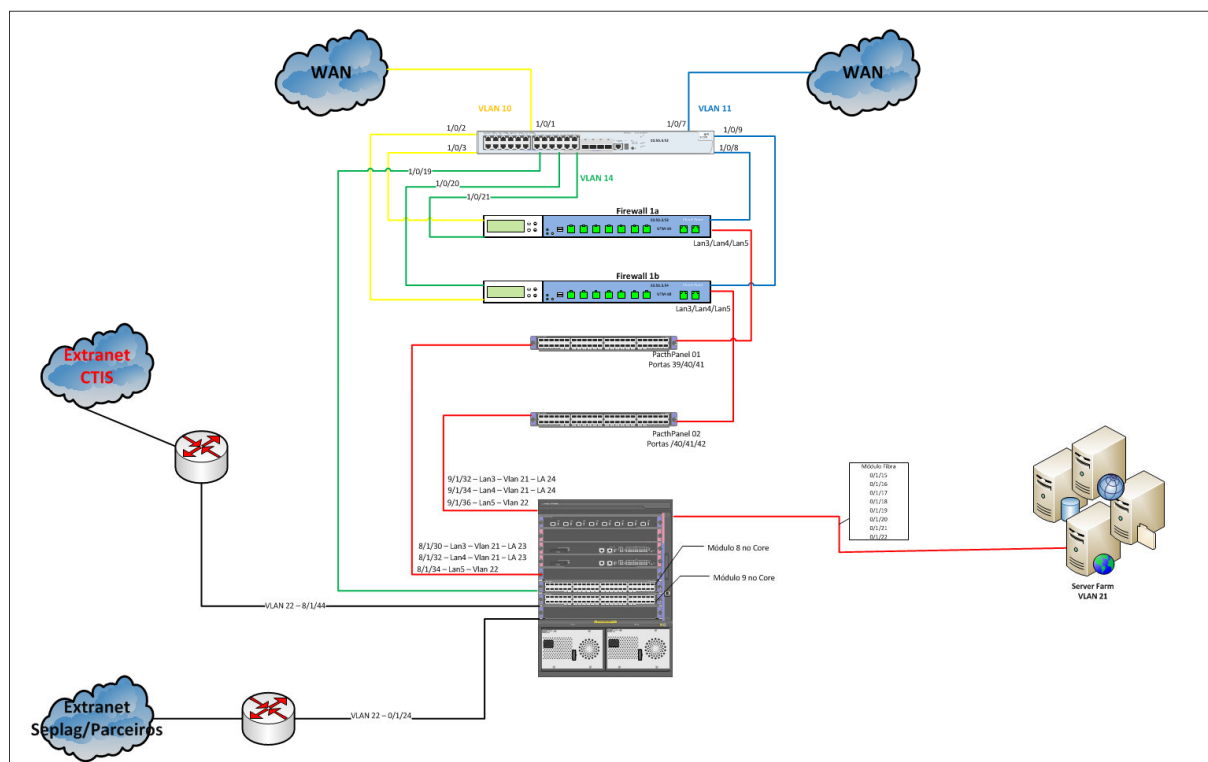
Figura 1 – Topologia lógica das conexões entre os *hosts* da rede da TERRACAP

LEGENDAS

| | |
|---|---|
|  | Host intermediário, em um caminho de rede que não foi escaneado |
|  | Host com menos de (3) três portas abertas |
|  | Host entre (3) três e (6) seis portas abertas |
|  | Host com mais de (6) seis portas abertas |
|  | Roteador, Switch ou ponto de acesso sem fio com menos de 6 portas abertas |
|  | Roteador, Switch ou ponto de acesso sem fio com mais de 6 portas abertas |
|  | Distância entre as conexões e o Host da rede |

5.3 Topologia Firewall

O quadro abaixo representa a distribuição lógica dos servidores e serviços relativos à política de segurança de determinados pontos da rede TERRACAP.



6. Teste de Intrusão e Vulnerabilidade

Para apoiar as futuras ações de melhoria que farão parte do Levantamento das Necessidades de TI e dos projetos elencados no PDTI foi executado um grupo de testes com o intuito de avaliar a possível existência de fragilidades no ambiente físico e lógico da TERRACAP. Esses testes foram realizados no período de 20, 23 e 24/04/2012 nas dependências da CODIN, no *DATACENTER* e na rede de dados do edifício sede da TERRACAP.

Para fins de avaliação da preocupação que se deve dedicar aos pontos avaliados, sugerimos a tabela abaixo como guia.

| Nível de Criticidade | Descrição |
|----------------------|--|
| Alta | Riscos mais altos à segurança do ambiente. Prioridade maior para uma solução corretiva em curto prazo. |
| Média | Riscos a segurança do ambiente que devem ter uma solução em médio prazo. |
| Baixa | Riscos a segurança do ambiente, que dependem de eventos com menor frequência, mas que também necessitam de solução em médio prazo. |

6.1 Teste ambiente físico

Para fins de contextualização, o ambiente físico é todo aquele que não envolve software e dados digitais. Desta forma, foram analisados os ambientes onde se encontram os equipamentos, como os móveis, ventilação, iluminação, acesso físico aos locais, os próprios equipamentos, dentre outros.

No ambiente físico encontraram-se algumas possíveis falhas que podem comprometer a segurança do ambiente. A descrição delas está agrupada na tabela abaixo:

| ID | Vulnerabilidade | Descrição | Criticidade |
|----|--|---|-------------|
| 1 | Controle de entrada de pessoal no edifício | Não existe um controle efetivo de pessoas que entram e saem do edifício. | Alta |
| 2 | Acesso físico aos servidores | A porta dos racks dos servidores possuem chaves, porém as portas ficam abertas. | Baixa |

| ID | Vulnerabilidade | Descrição | Criticidade |
|----|--|---|-------------|
| 3 | Acesso aos switches do DataCenter | O acesso aos switches do DataCenter feito por biometria. | Baixa |
| 4 | Tipo de condicionamento de ar do DataCenter | O ar-condicionado do DataCenter não é apropriado, a humidade residual do ar pode danificar os equipamentos a longo prazo. | Média |
| 5 | Monitoramento das câmeras de segurança | Não existe um monitoramento efetivo das câmeras de segurança do edifício. | Alta |
| 6 | Contingência de energia no ar-condicionado do DataCenter | O ar-condicionado do DataCenter não funciona após uma queda de energia na rede. | Alta |
| 7 | Histórico no acesso ao DataCenter | Há um histórico de acesso ao datacenter para uma possível auditoria. | Baixa |
| 8 | Material comburente na sala segura | A sala segura do DataCenter possui materiais comburentes. | Baixa |

6.2 Teste ambiente lógico

No ambiente lógico foram analisados *softwares* e ferramentas digitais utilizadas no ambiente virtual da TERRACAP. Os testes restringiram-se à rede de servidores no range de IP 10.50.3.0.

Nesse contexto, apresentaram-se algumas possíveis falhas que podem comprometer a segurança do ambiente, quais sejam:

| Produto/Serviço | Descrição | Criticidade |
|-----------------|--|-------------|
| VMWare | Versão 5.0 | Baixa |
| SSH | Foram encontrados 62 servidores com o serviço SSH habilitado. É necessário verificar versões abaixo de 5.5 | Média |
| RDP | 31 hosts foram encontrados com o protocolo habilitado. | Média |
| IIS httpd | Hosts na versão 7.5 do IIS devem ser verificados, | Alta |

| Produto/Serviço | Descrição | Criticidade |
|-----------------|--|-------------|
| | informações em: http://www.securityfocus.com/bid/36935 | |
| Linux | Versões 2.4.x, 2.6.9 até 2.6.27 foram encontradas. Muitas versões da série 2.4.x e anteriores a 2.6.18 possuem rootkits. | Média |
| MS Windows* | Vulnerabilidades do Windows são bem frequentes. Atenção especial para essa: http://www.securityfocus.com/bid/52353 | Alta |

*As vulnerabilidades do Windows devem ser verificadas periodicamente

Não se realizaram provas de conceito para tais vulnerabilidades, pois estão excluídas do escopo. As máquinas que precisam de uma maior atenção estão ilustradas nas bordas da figura 1 do item 5.2 deste documento.

7. Considerações

A infraestrutura de rede da TERRACAP está segmentada em *switchs* ligados em pilha na topologia estrela. Tal rede é estruturada, usa cabeamento *CAT6*, possui dois *Links* Internet de 17MB (Embratel fibra ótica) e uma ligação com a rede *GDFNet* via fibra ótica *Gigabit*. Além disso, sua rede elétrica está estabilizada em 110v no edifício sede, onde se situa o *DATACENTER*, e seu *NOBREAK* pode durar até 1h30min após a falta de energia fornecida pela concessionária.

A complexidade de instalações para infraestrutura de TI em qualquer empresa é algo que deve ser planejado, implantado e gerenciado com bastante cuidado, visto que dela dependem todas as outras iniciativas tecnológicas ligadas ao gerenciamento da informação. O levantamento preliminar aqui apresentado será parte integrante do PDTI e será novamente abordado nas fases de desenvolvimento do plano, buscando evidenciar sugestões de melhoria e boas práticas de mercado para o melhor gerenciamento dos ativos de infraestrutura e segurança.

8. Execução e Aprovação

Executado por:

Luciano Simões de Almeida
Consultor de TI
Allen Rio Informática

Aprovado por:

Geraldo Rodrigues Soares
Coordenador de Informática/CODIN

Romildo Ribeiro dos Santos
Chefe da Divisão de Sistemas
Executor do Contrato 135/2011

Data da emissão: 20/04/2012