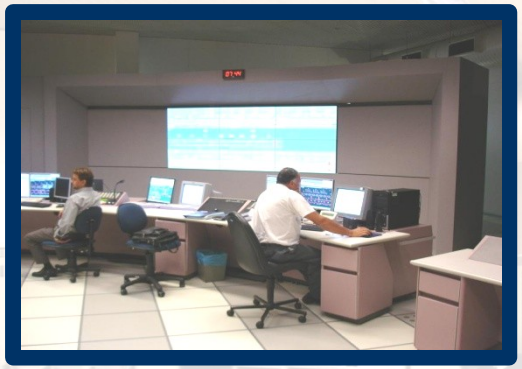
Segurança da Informação aplicada em CCO



Objetivo

- **Este trabalho tem como objetivo descrever uma metodologia de segurança da informação aplicada às redes de computadores em Centros de Controle Operacional.**

Definição de Centro de Controle Operacional

- O Centro de Controle Operacional ou CCO também conhecido como centro nervoso ou cérebro central é um local físico onde são feitas a supervisão e o controle operacional centralizado.

Áreas de Aplicações de Centro de Controle Operacional

- O Centro de Controle Operacional pode ser utilizado em diversos setores, tais como transporte, energia, saneamento básico, meio ambiente, segurança, indústria, petróleo, gás, etc.

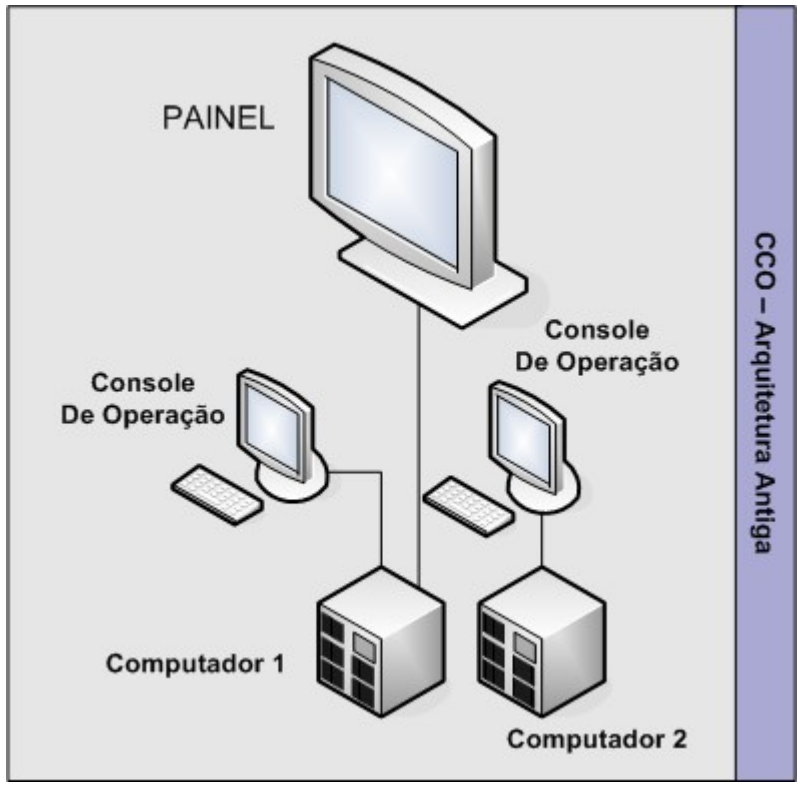
Composição Básica do Centro de Controle Operacional

- Composto por consoles de operação e seus respectivos operadores, painéis mímicos, redes de comunicação e computadores.

Histórico

- O Centro de Controle Operacional sofreu grandes mudanças após o aparecimento dos computadores.
- Antes disso, as conexões com os equipamentos do sistema controlado eram implementadas diretamente através de fios.
- Há aproximadamente 50 anos, com o início da produção em série de computadores, a arquitetura do Centro de Controle foi se alterando.

Histórico

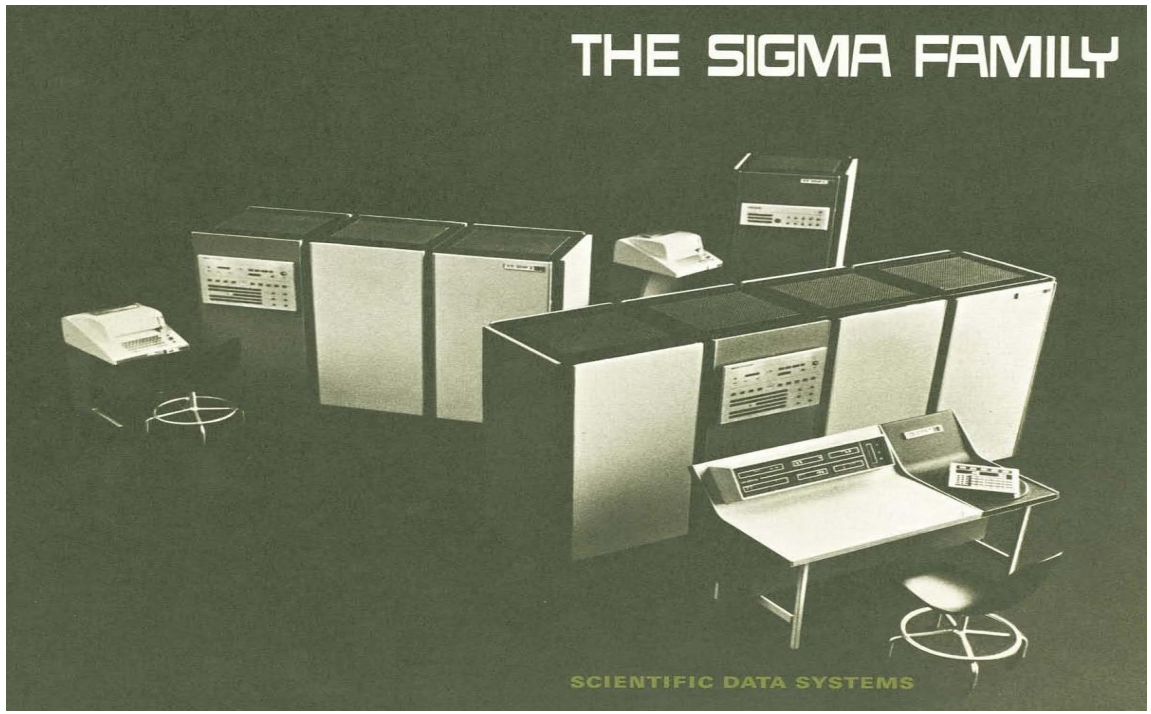

PAINEL
Console
De Operação
Console
De Operação
Computador 1
Computador 2
CCO – Arquitetura Antiga

Histórico

1959 - CCO na área de Geração de Energia
Computador PRODAC

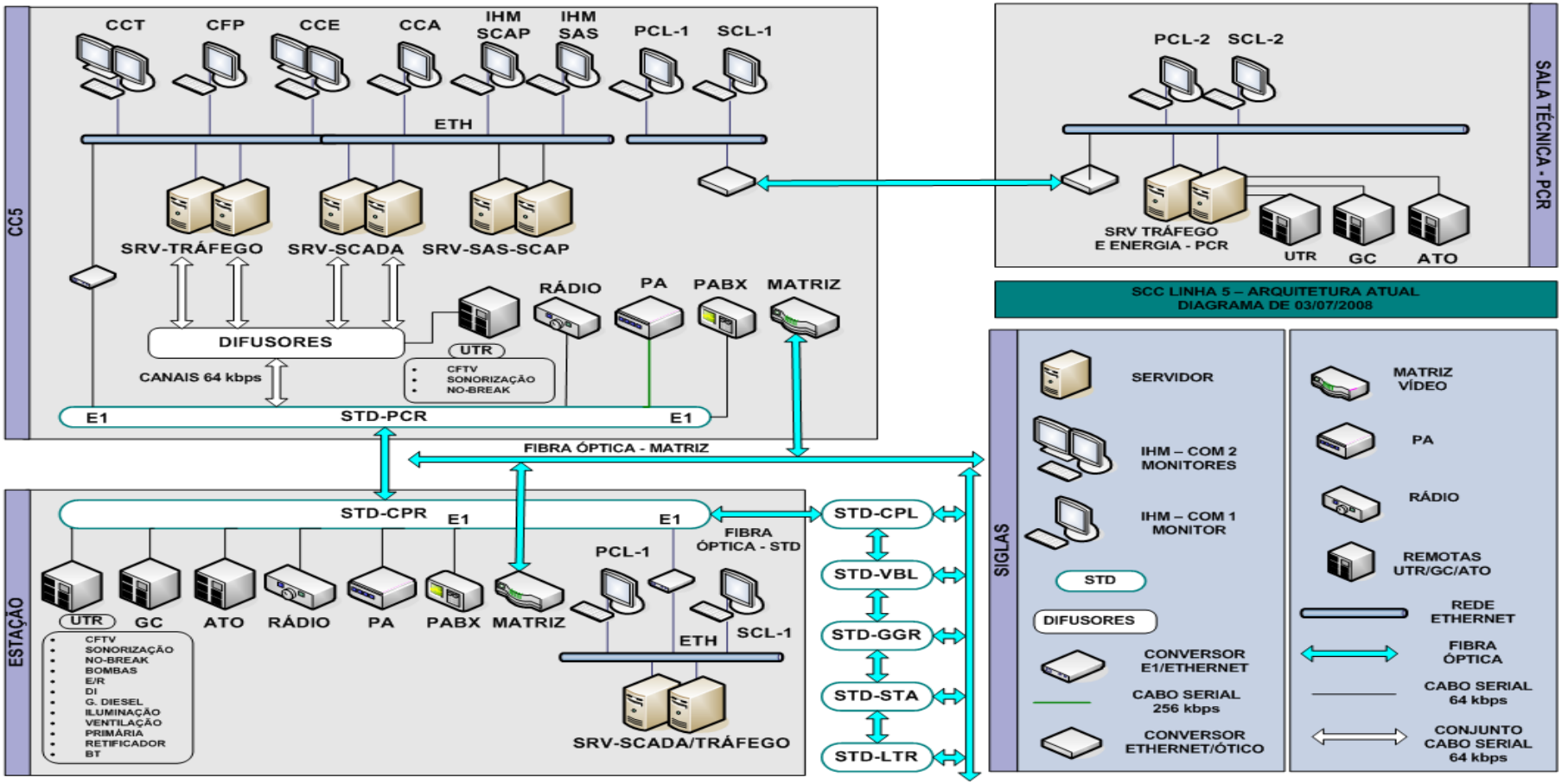
Histórico

- Familia de Computadores Sigma - SDS



Segurança da Informação aplicada em CCO

Arquitetura Distribuída



Arquitetura Distribuída

- CCO BART com arquitetura distribuída.

Arquitetura Distribuída

- CCO da Reliance Infocomm – Índia

Arquitetura Distribuída

- CCO da ARACOM – Arábia Saudita

Arquitetura Distribuída

- CCO do tráfego viário de Tóquio – Japão

Eventos Importantes

- 1959-CCO na área de Geração de Energia - computador PRODAC
- 1967-Primeira implantação de sistema P250-Westinghouse
- 1972-CCO Metrô BART 1ª Linha Freemont –computador P250
- 1974-CCO Metrô de São Paulo –Linha 1 Azul – computador P250
- 1982-Arquitetura distribuída
- 1999-BS-7799-2 – Criação da norma ” Information Security Management Systems - ISMS”
- 2005-ISO/IEC 27001 – Substituição da norma BS-7799-2 -ISMS

Riscos de Segurança

- Com a larga utilização das redes de computadores nos centros de controle, os riscos relacionados à segurança da informação se tornaram maiores podendo comprometer a disponibilidade projetada para o sistema e a confidencialidade e a confiabilidade dos dados operacionais.

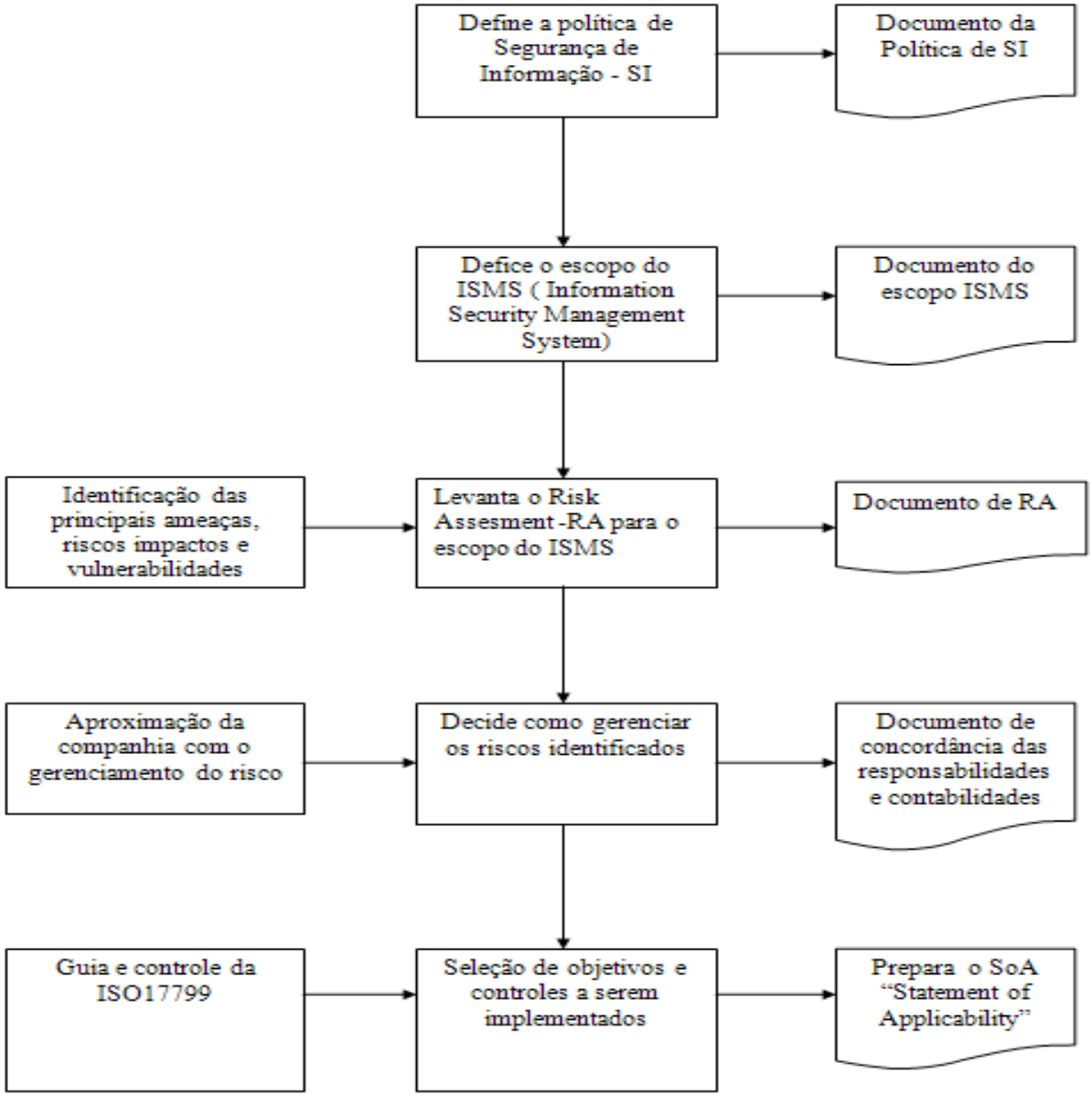
Riscos de Segurança

- Várias medidas poderiam ser adotadas para implementação da Segurança da Informação, porém, quando avaliamos que o prejuízo poderá ser grande caso ocorra um problema de segurança, se faz necessário então uma avaliação mais detalhada dos pontos que envolvem a SI, sem que estas medidas engessem o processo. Portanto, é necessário fazer uma análise do quadro atual, aplicando as normas conforme a necessidade e o grau de importância do negócio.

Sistema de Gerenciamento de SI - ISMS

- Quando a empresa já possui uma certificação ISO-9000, OHSAS-14000, será mais fácil adotar uma metodologia de trabalho em cima de uma norma relacionada à Segurança da Informação que irá facilitar o processo de implantação da Política de Segurança da Informação, sem no entanto haver a necessidade de se certificar.

Fluxograma ISO - 27001



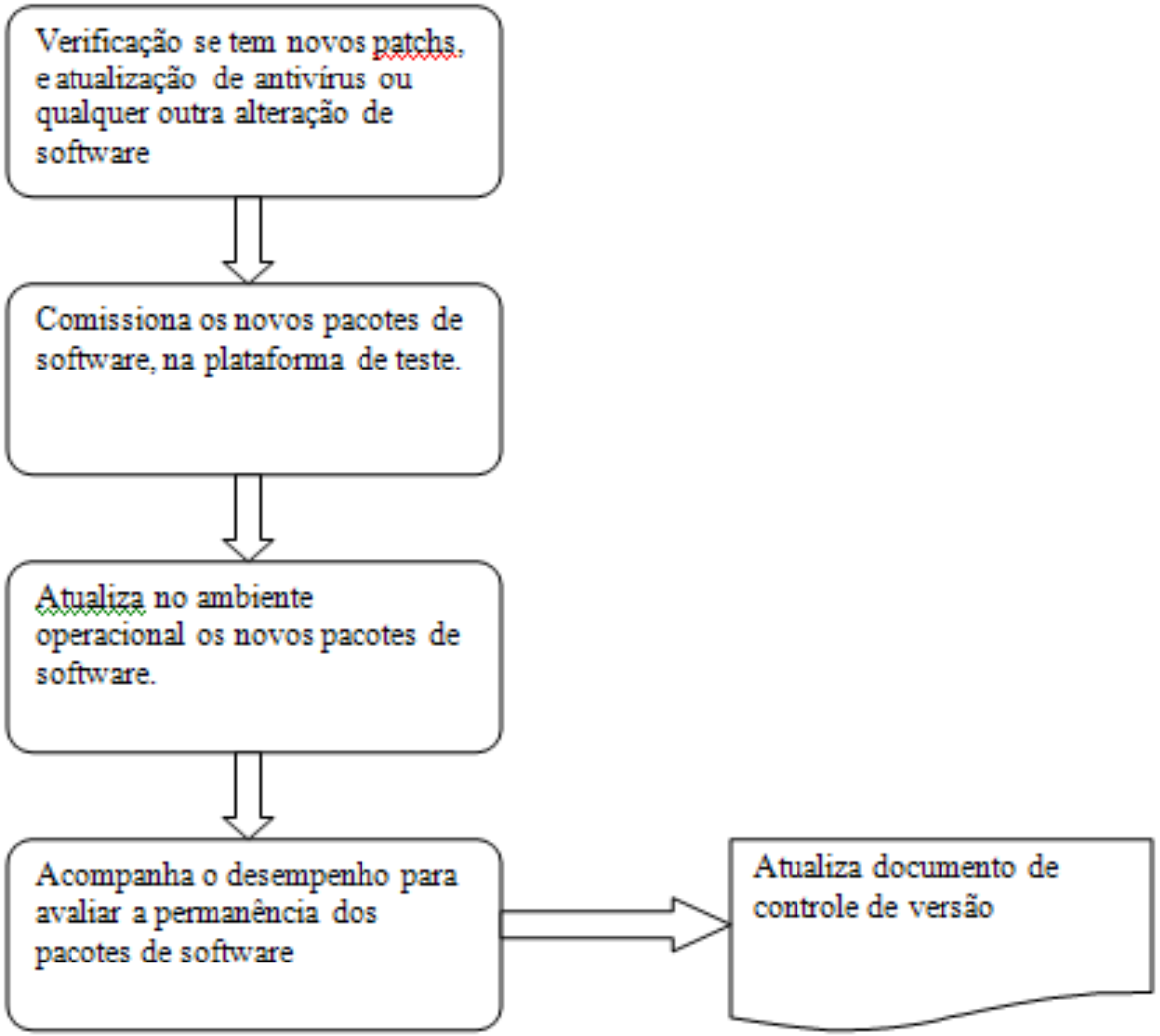
Práticas de Segurança

- Necessidade de entrada de login para uso dos recursos da rede.
- Firewall entre as redes de controle e a rede corporativa.
- Manter atualizado o antivírus e os patchs do sistema operacional.
- Proteção ao dado que trafega na rede através de protocolos seguros e criptografia.
- Cada computador da rede deve possuir uma proteção mínima individual.

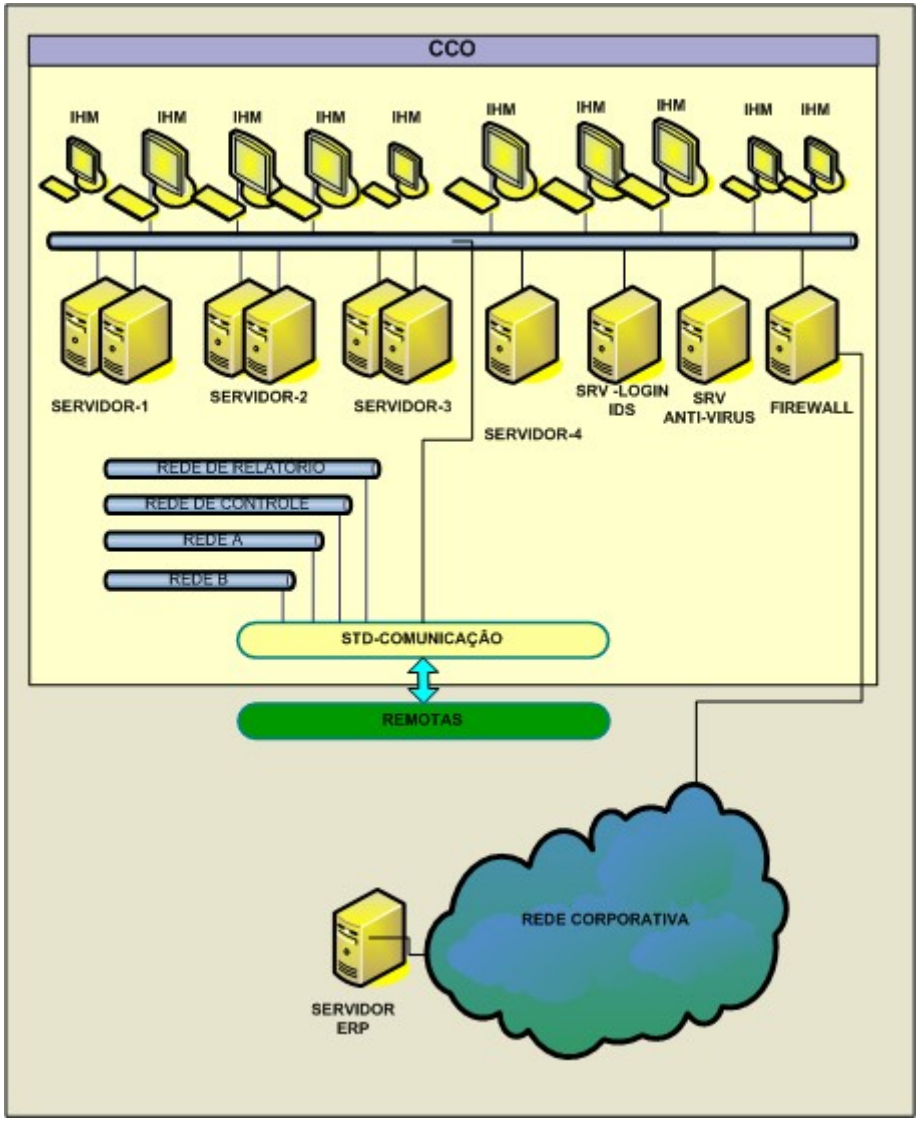
Práticas de Segurança

- **Importante: O item anterior referente ao antivírus e patchs deve ser comissionado em plataforma de teste antes de ser inserido no ambiente operacional.**

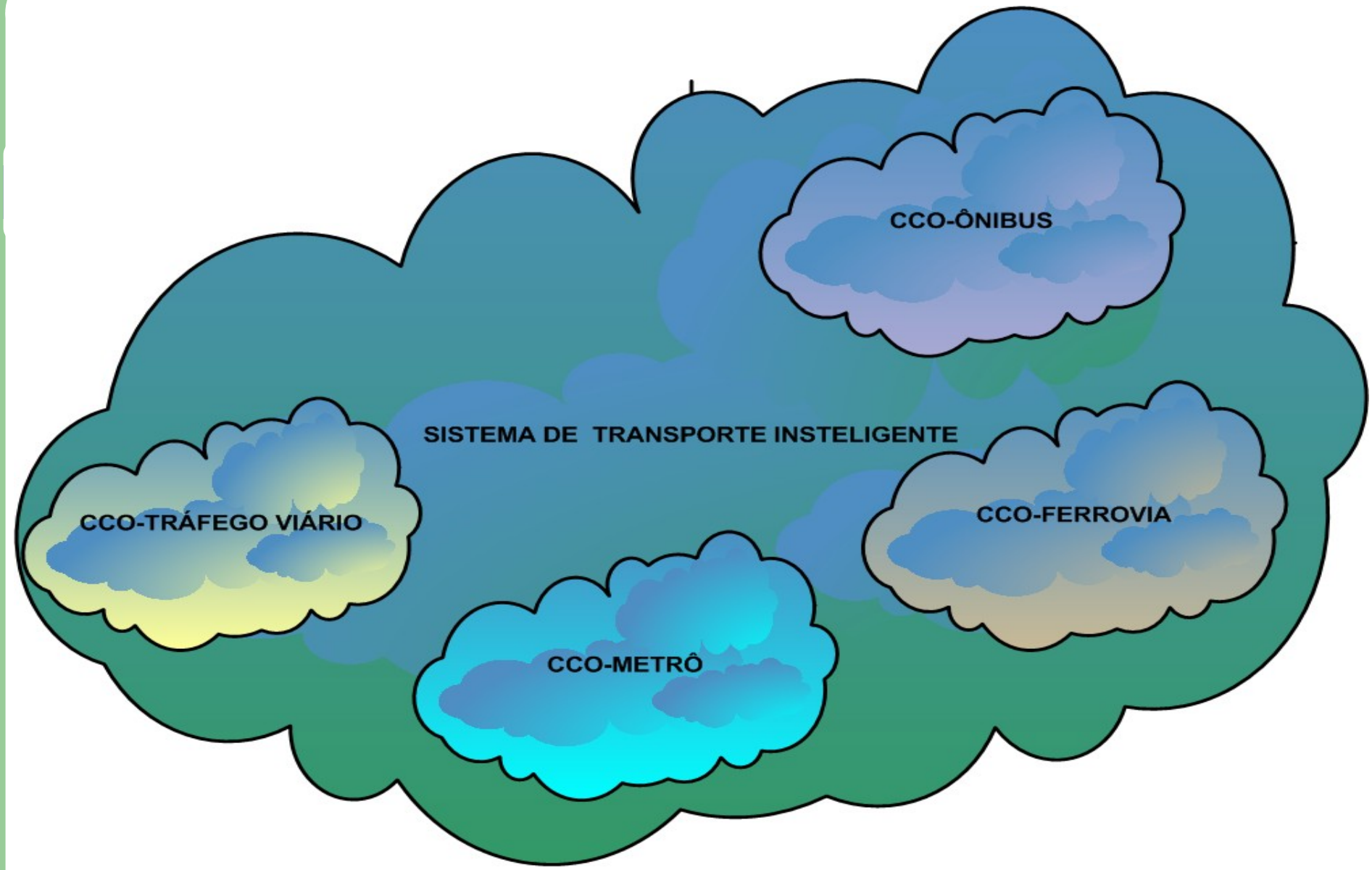
Rotina de Atualização de Software



Exemplo de Arquitetura de CCO



Exemplo de Arquitetura Integrada



Conclusão

- Podemos afirmar com certeza que a vulnerabilidade do sistema, após a implementação do ISMS, diminui sensivelmente, garantindo através de riscos calculados a disponibilidade, a integridade e a segurança da aplicação e da informação.

Conclusão

- **É imprescindível a disponibilização das informações operacionais em tempo real para a rede corporativa exportando os dados operacionais para o servidor ERP da empresa, ou até mesmo se integrando com outros Centros de Controle.**

Segurança da Informação aplicada em CCO

Conclusão

- Podemos afirmar que os Centros de Controle irão proliferar como nunca aconteceu antes, pois a otimização através da operação centralizada é questão de sobrevivência para vários setores e, como vimos anteriormente, tem um papel fundamental na integração entre vários serviços essenciais ao cidadão Metropolitano. Portanto para que isto ocorra, as implementações de segurança da informação deverão estar implantadas para que esta integração não venha causar efeitos colaterais ao sistema operacional.

FIM

OBRIGADO PESSOAL

Marcos Spigliatti
email: spig@metrosp.com.br