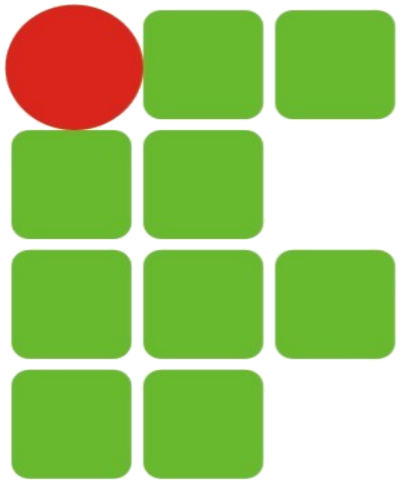
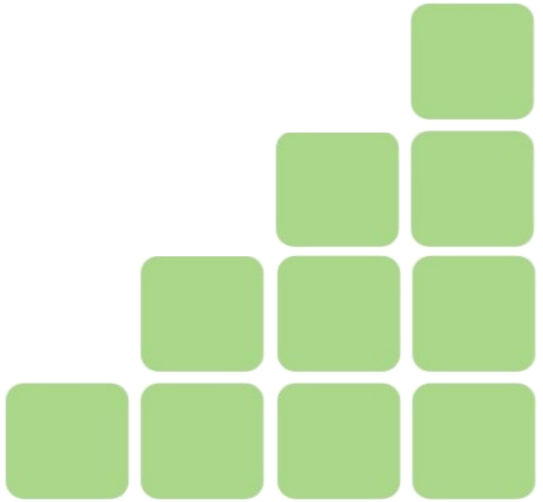


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Estado da Arte da **(in)Segurança da Informação** em Soluções de **Automação Hospitalar**

14/05/2010

Ricardo Kléber M. Galvão
ricardo.galvao@ifrn.edu.br



Realidade da Saúde Pública no Brasil

Fundação Instituto de Administração (FIA)/USP (2008)

- "(...) simplesmente colocar mais dinheiro dificilmente resolve os problemas. O aporte de recursos é condição necessária, mas não suficiente, pois a nossa carência mais latente está relacionada à **gestão**"
- "Se a gente investe um número semelhante à média da região e os nossos indicadores são consistentemente piores, há alguma coisa errada sobre a forma como estamos gerindo esses recursos."

- os gastos em saúde vêm aumentando praticamente em todo o mundo nos últimos anos, tanto em função do envelhecimento da população, como pela **incorporação de novas tecnologias.**

Leandro Fraga
(um dos coordenadores da pequisa)

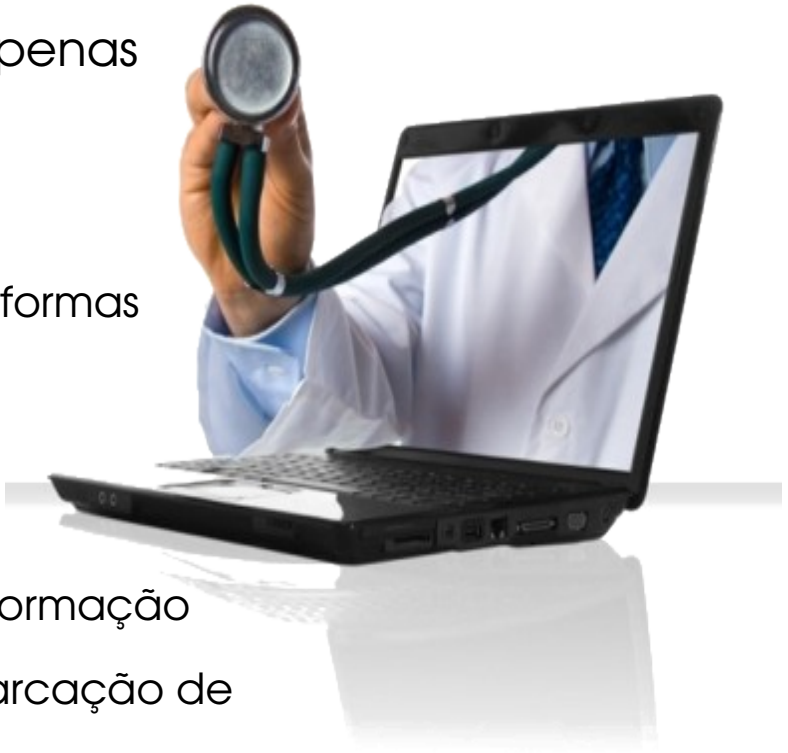
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Automação Industrial

- Uso de novas tecnologias na automatização de processos manuais;
- Manipulação de grandes volumes de dados/informações;
- Rapidez e confiabilidade nas respostas (análise de dados/equipamentos);
- Identificação e disponibilização de informações relevantes;
- Estrutura de Comunicação ampla, adaptável e acessível;
- Gerenciamento eficaz;
- Integração de **Equipamentos, Sistemas e Pessoas**;
- **Confiabilidade (!!??);**
- **Segurança (!!??)**

Automação Hospitalar

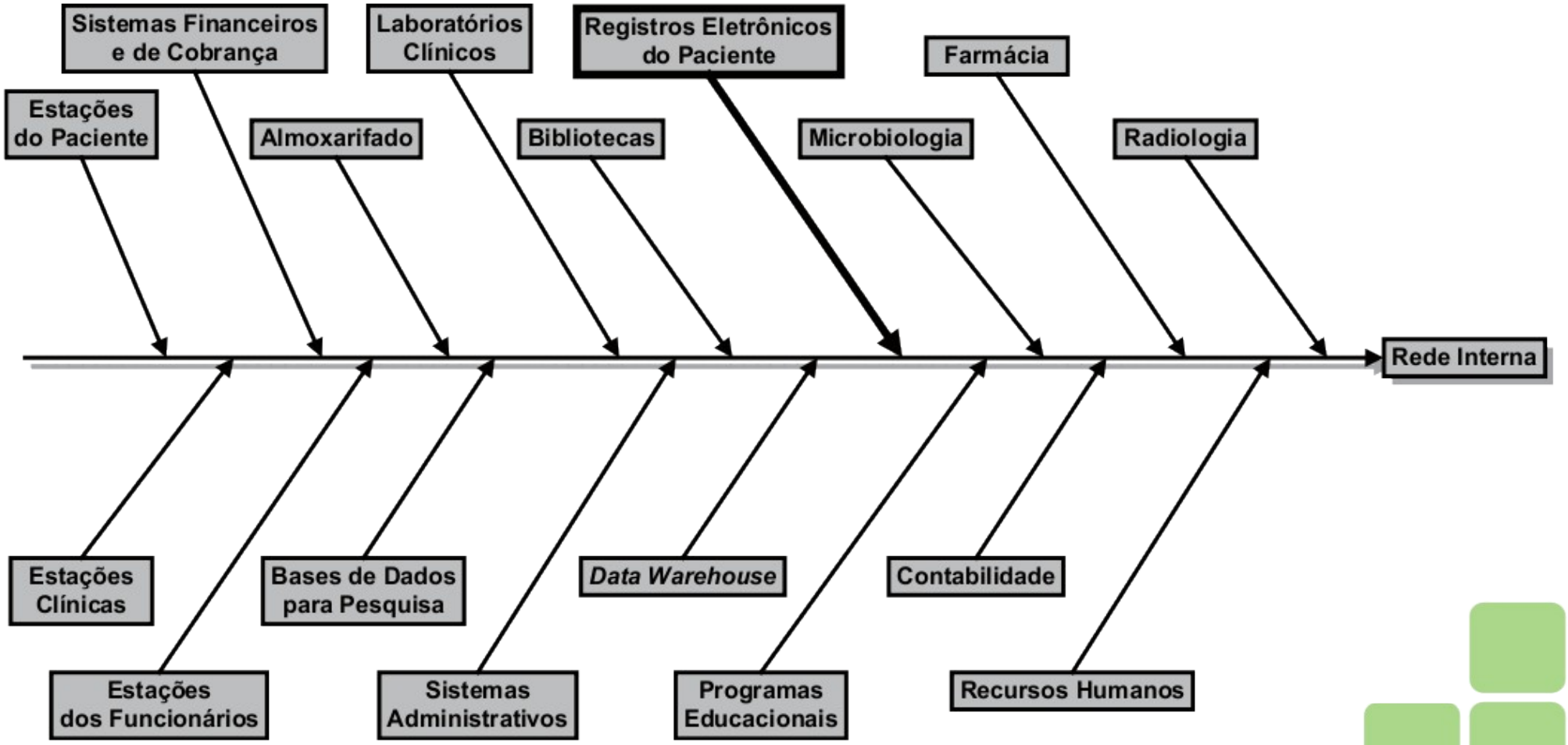
- Área hospitalar pouco automatizada (ações em apenas parte dos processos)
- Área multidisciplinar
  - Envolve linguagens de programação (software), plataformas eletrônicas (hardware), atuação (mecânica) e fluidos fármacos (formas de medicação).
- Perspectivas:
  - Rede de Informações: Composta pelos sistemas de informação utilizados na área hospitalar (prontuário eletrônico, marcação de consultas, sistemas de internamento, sistemas de laboratório e similares);
  - Rede de Controle: Composto pelos sistemas utilizados para o monitoramento de pacientes.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

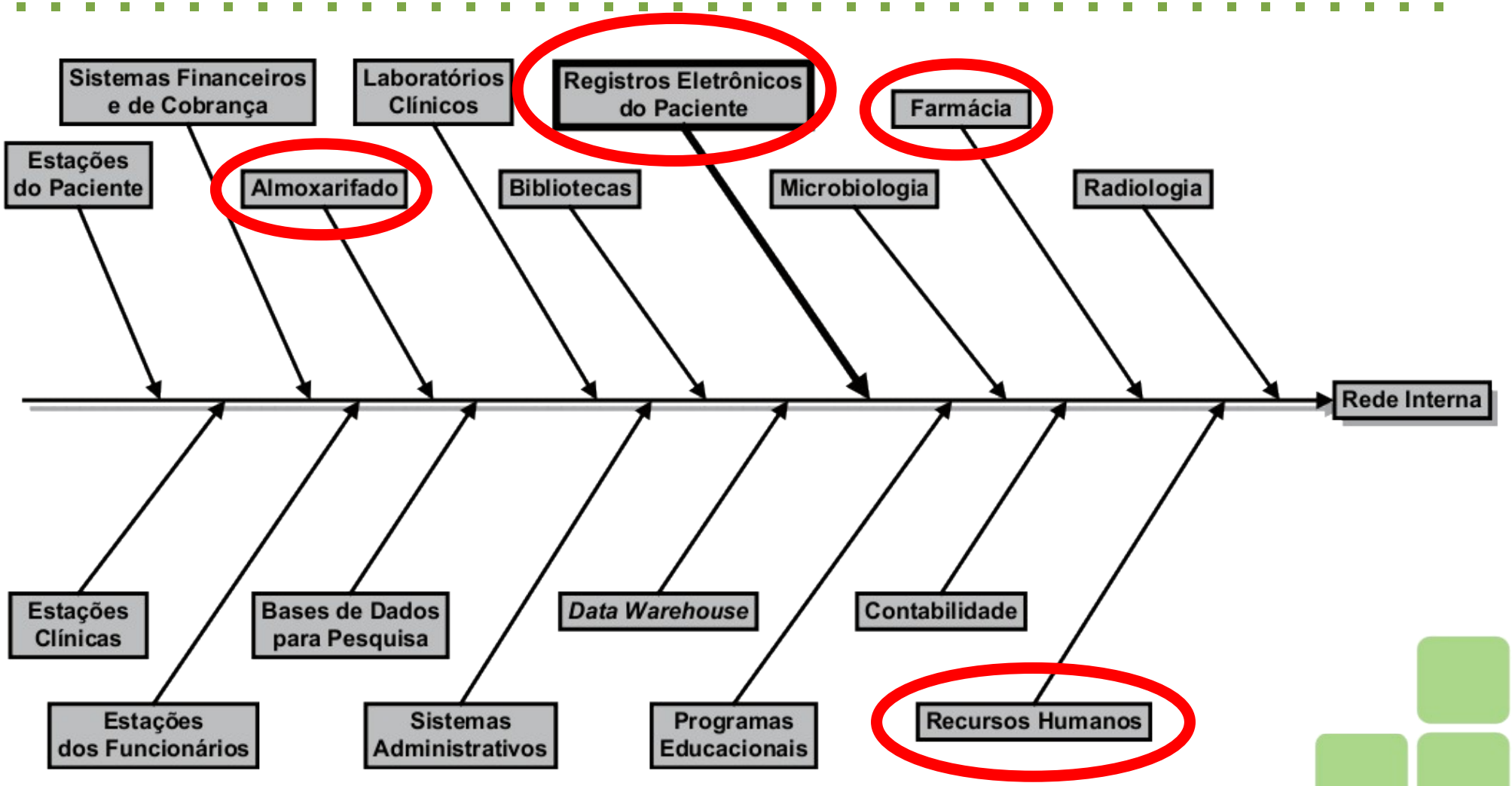
Automação Hospitalar :: Abrangência ?

Automação Hospitalar



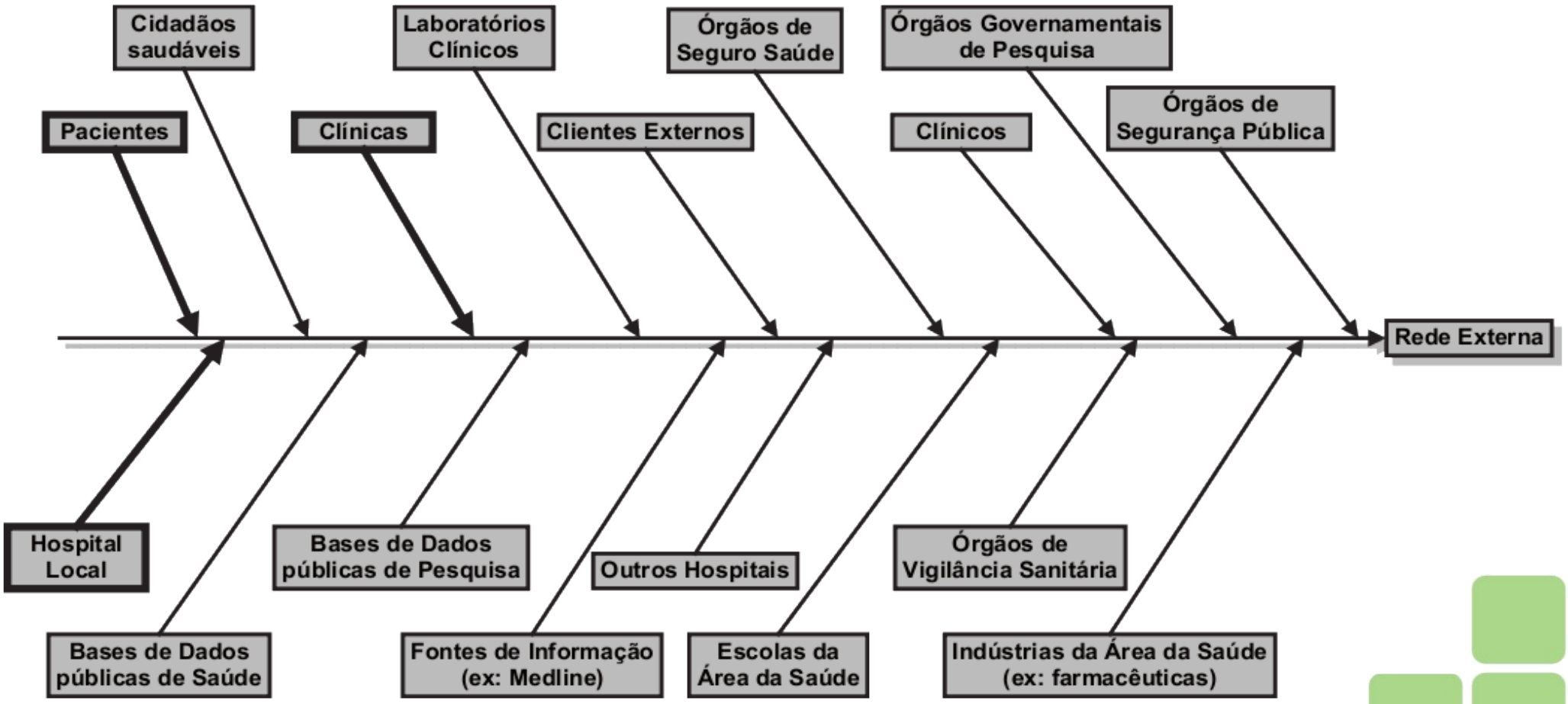
Rede Interna

Automação Hospitalar



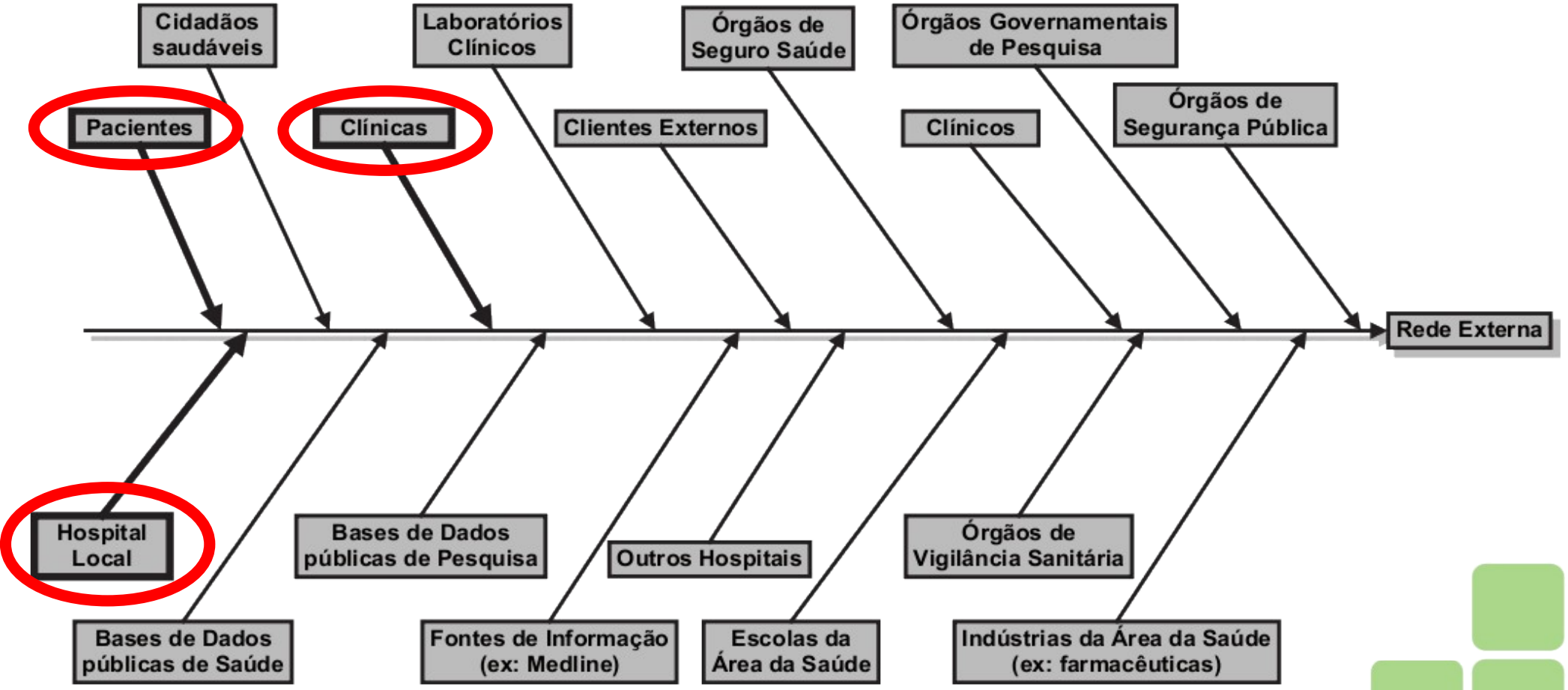
Rede Interna

Automação Hospitalar



Rede Externa

Automação Hospitalar



Rede Externa

Automação Hospitalar

- Escopo desta apresentação
  - **Rede Interna:**
    - Pacientes, Equipe Médica, Equipamentos, Almoxarifado, Medicamentos
  - **Rede Externa:**
    - Pacientes, Hospitais/Clínicas
- Foco Principal: Soluções de **Identificação** e Rastreio de Pessoas e Objetos
  - Problemas relacionados à **segurança** nestes processos

Problemas **não** abordados nesta apresentação

- *armazenamento de informações e backups seguros;*
- *tolerância a falhas e mecanismos de recuperação;*
- *segurança de software (sistemas operacionais seguros e sistemas auditáveis);*
- *segurança de hardware (genéricos e específicos);*
- *segurança física (controle de acesso e prevenção de acidentes);*
- *métodos gerenciais para definição, estabelecimento e implantação de políticas e procedimentos de segurança;*
- *resistência em utilizar ou confiar em sistemas computadorizados;*
- *geração e manutenção de senhas;*
- *treinamento e atualização de usuários;*
- *manutenção e administração de sistemas (hardware e software);*
- *vírus e similares (trojans, etc.);*
- *erros humanos de entrada de dados*
- *...*

Motivo Principal: Contribuição ao Foco do Evento

Automação Hospitalar

- Aplicações (Específicas)
  - Monitoramento de Equipamentos
  - Monitoramento de Pacientes, Médicos, Enfermeiros e Equipes de Apoio
  - Identificação e Controle de Pacientes
  - Identificação de Funcionários e Controle de Acesso
  - Pedigree Eletrônico (e-Pedigree) :: Controle de Medicamentos
  - Prateleiras Inteligentes
  - ...

Automação Hospitalar

Quiosque Hospitalar

Automação Hospitalar

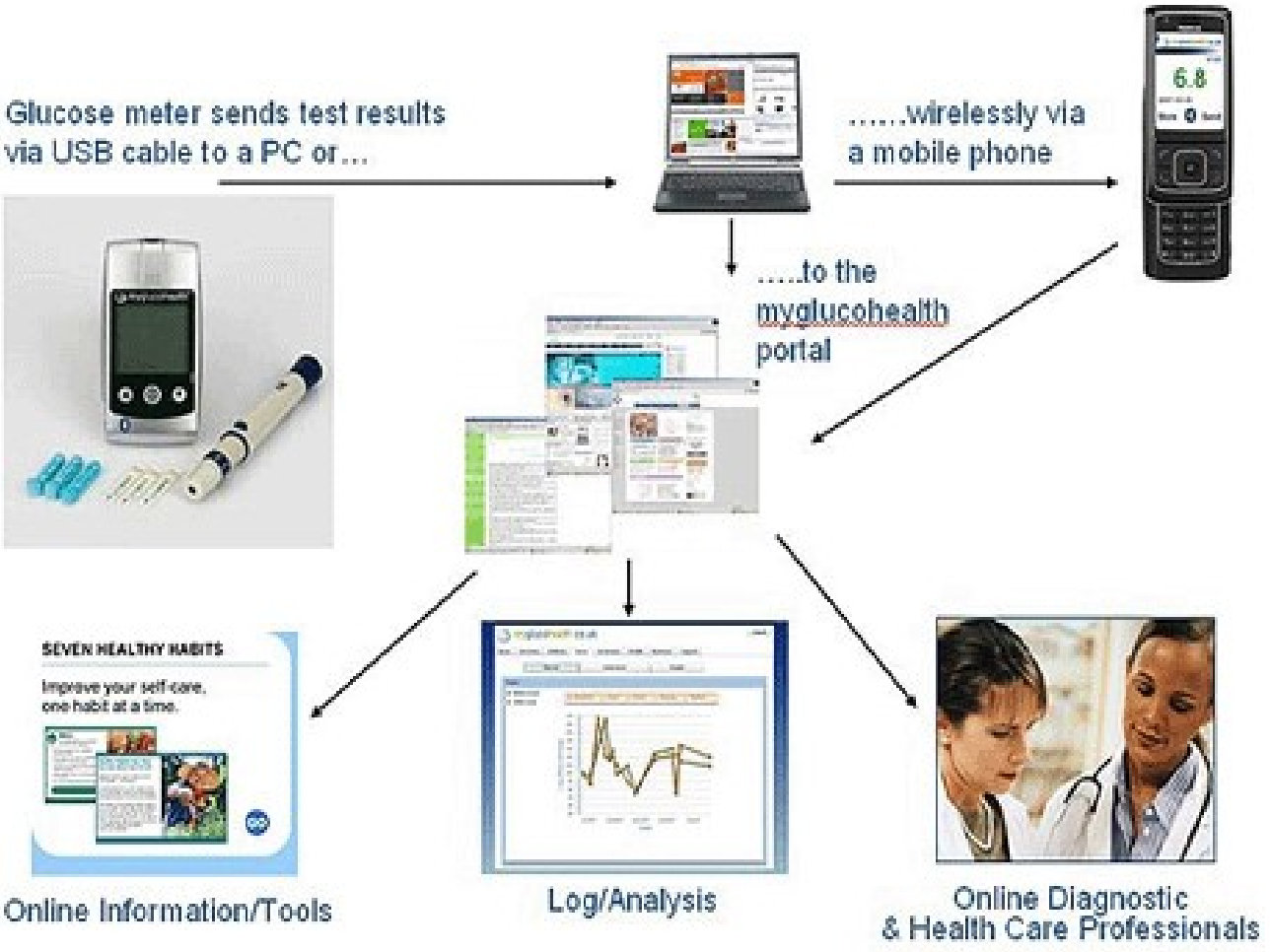
5-Right's Application

- Passive Tags
- Dual RFID & Barcode
- PDA's & Tablet PC's
- Wireless database access

(Images provided by St. Clair Hospital, Pittsburgh, PA)

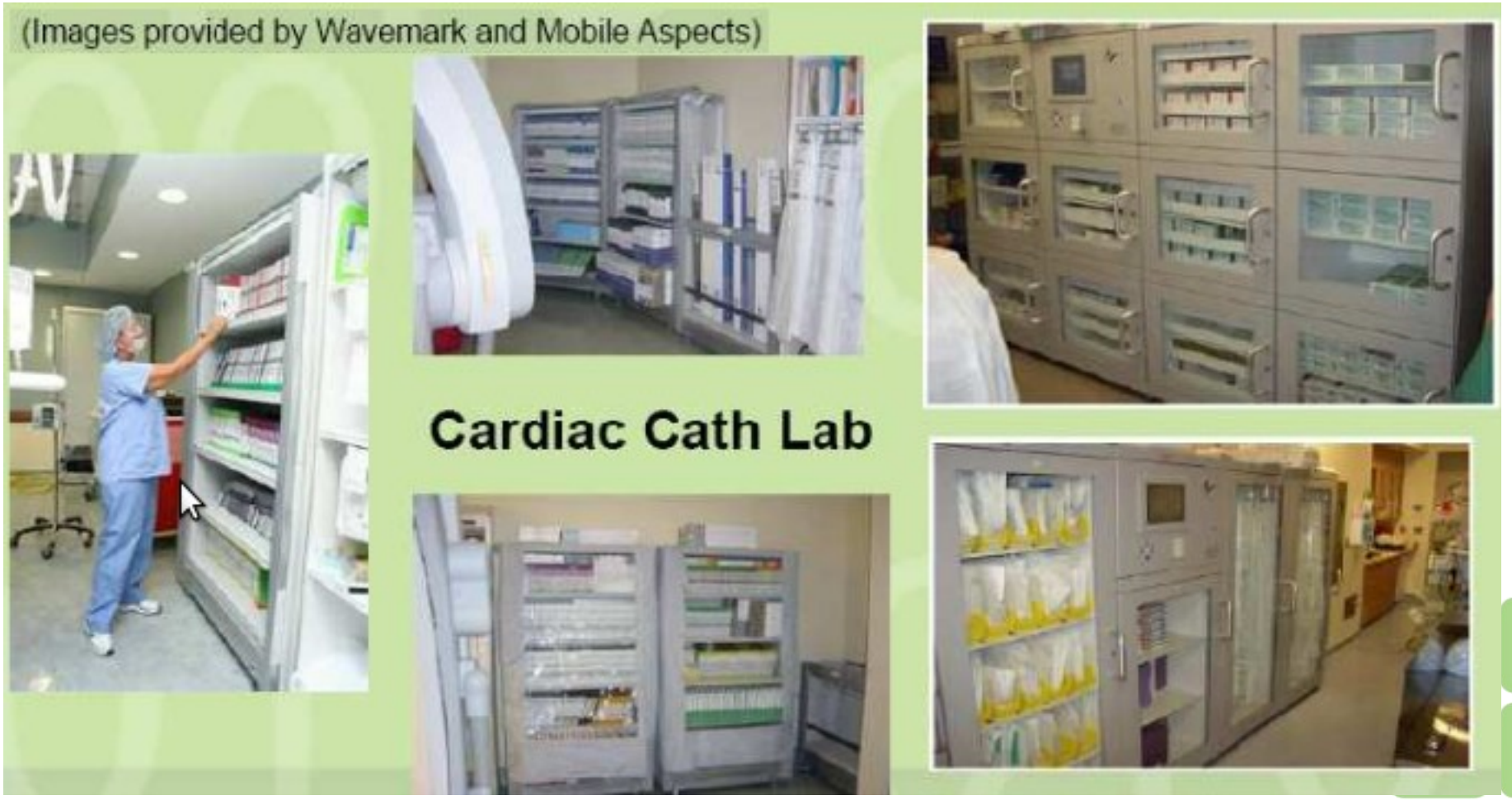
Identificação de Pacientes (Pulseiras)

Automação Hospitalar



Monitoramento de Diabéticos

Automação Hospitalar

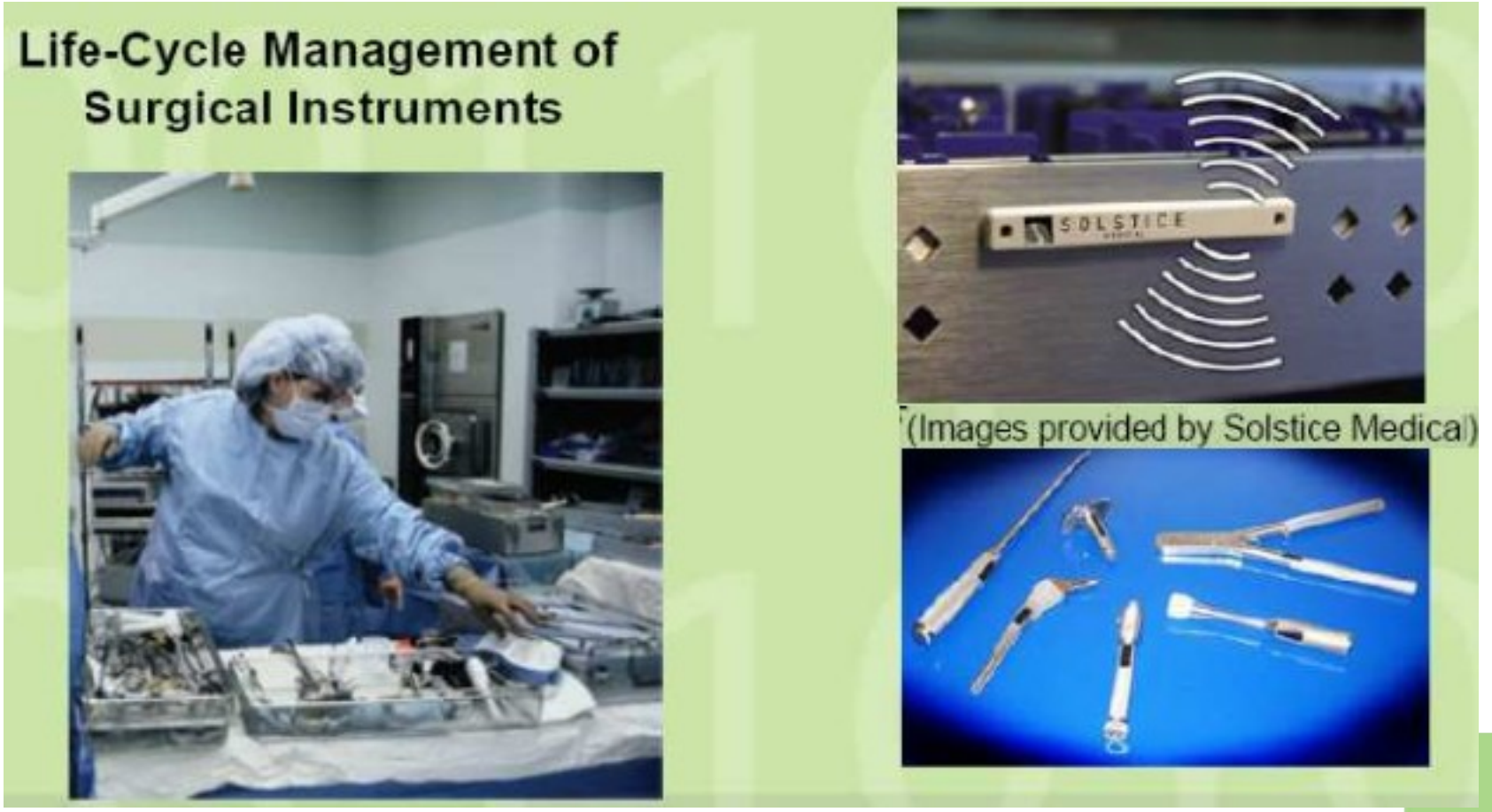


Prateleiras Inteligentes

Automação Hospitalar

Gerenciamento de Arquivos

Automação Hospitalar



Gerenciamento de Equipamentos

Automação Hospitalar

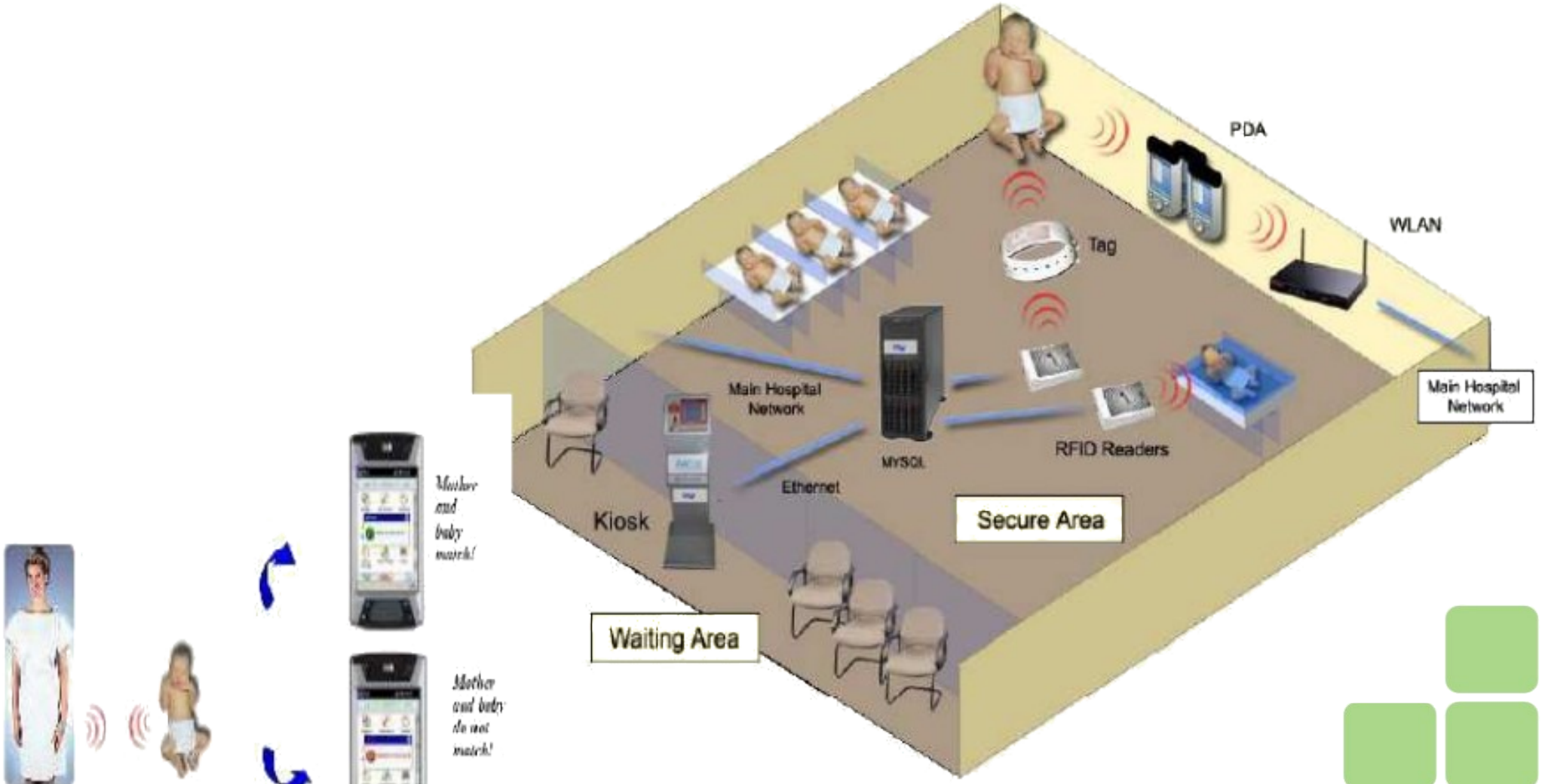
Banco de Sangue

Automação Hospitalar

Gerenciamento de Leitos

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

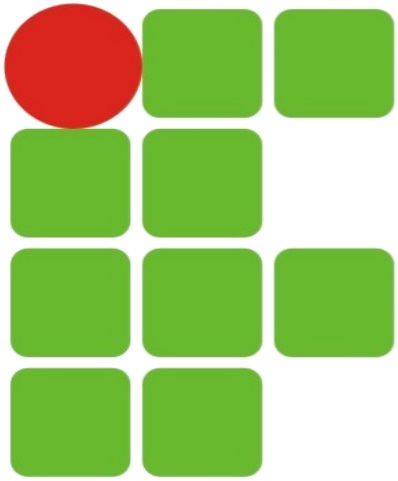
Automação Hospitalar



UTI Neo-Natal

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Finalmente...



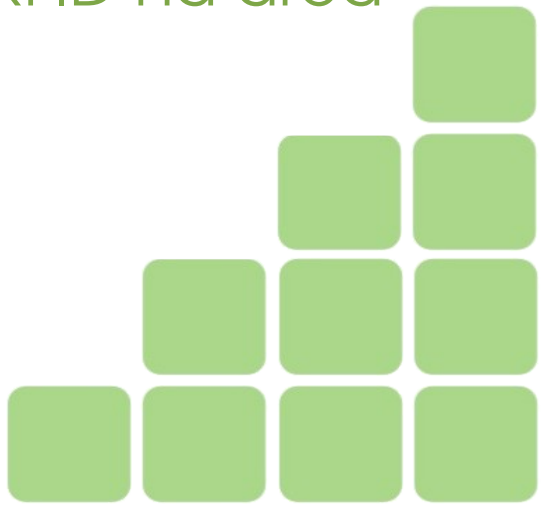
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Estado da Arte da **(in)Segurança da Informação** em Soluções de Identificação Baseadas em RFID na área de **Automação Hospitalar**

14/05/2010

Ricardo Kléber M. Galvão
ricardo.galvao@ifrn.edu.br

REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2009



Automação Hospitalar / Brasil / Rio Grande do Norte

UFRN

UERN

LAHB

Laboratório de Automação Hospitalar e Bioengenharia

LSI Laboratório de Sistemas Inteligentes

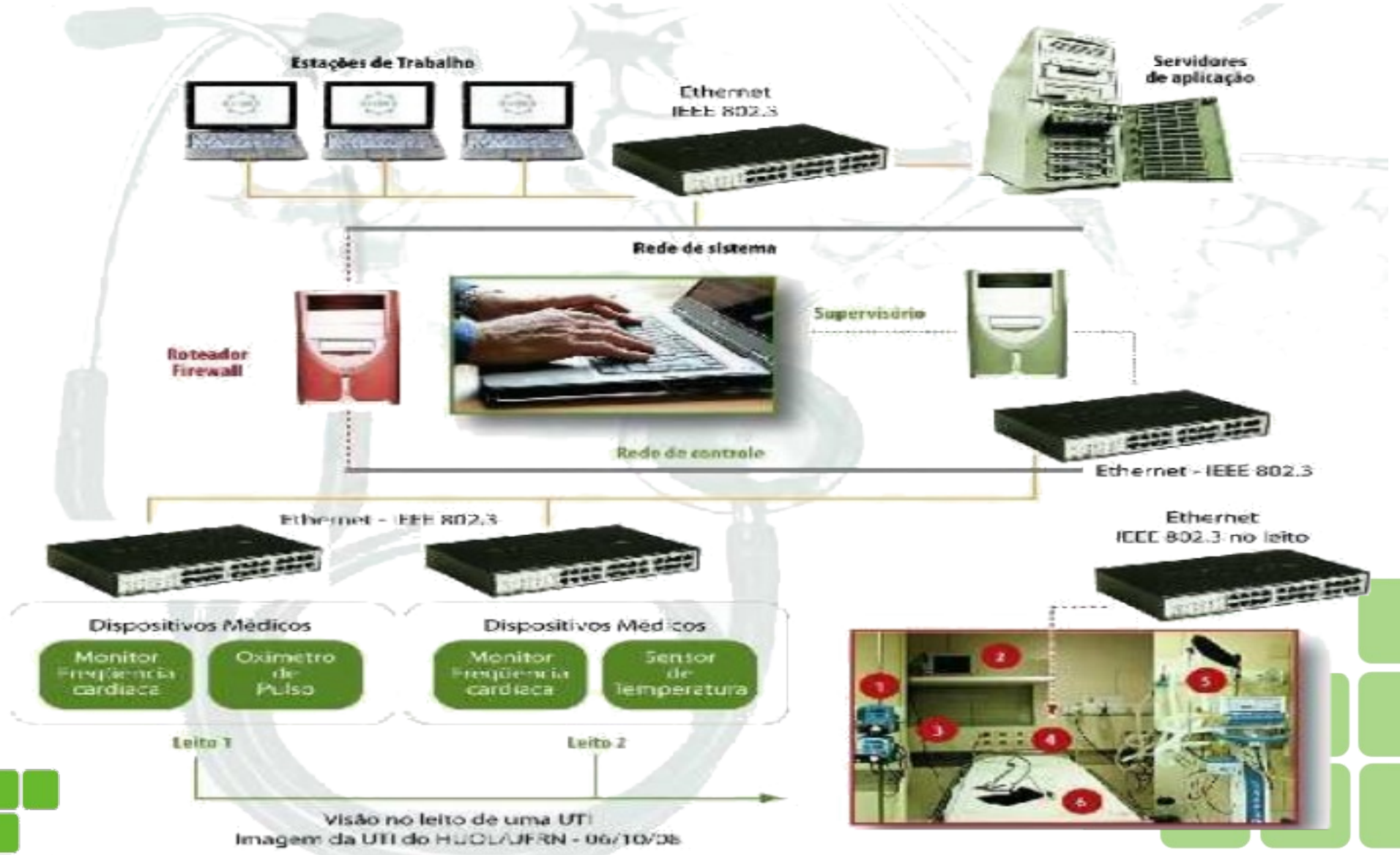
LES Laboratório de Engenharia de Software

HUAB

GOVERNO DO ESTADO DO RIO GRANDE DO NORTE
Secretaria de Estado da Saúde Pública

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Automação Hospitalar / Brasil / Rio Grande do Norte



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

HUAB

Automação Hospitalar / Brasil / Rio Grande do Norte

Smart Cards armazenam informações de seus usuários (médicos, enfermeiros e pacientes)

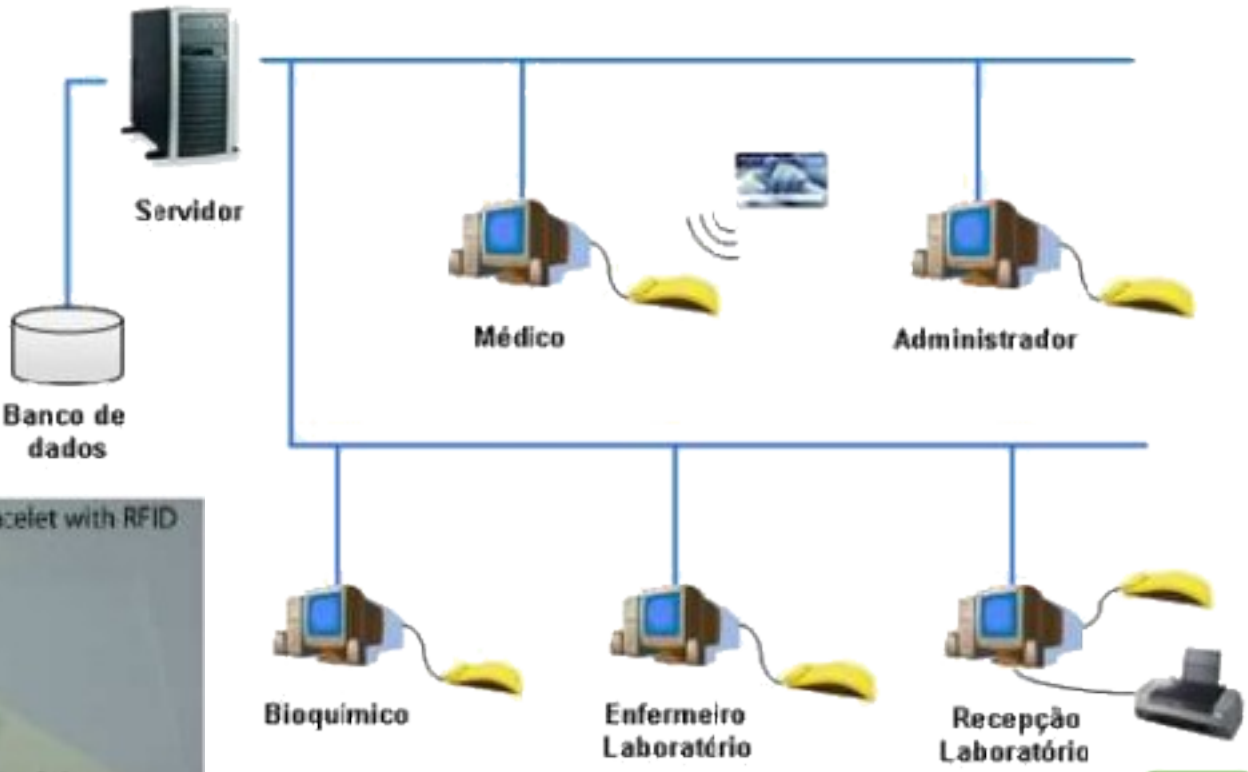
Médico

Enfermeira

Pacientes

Automação Hospitalar / Brasil / Rio Grande do Norte

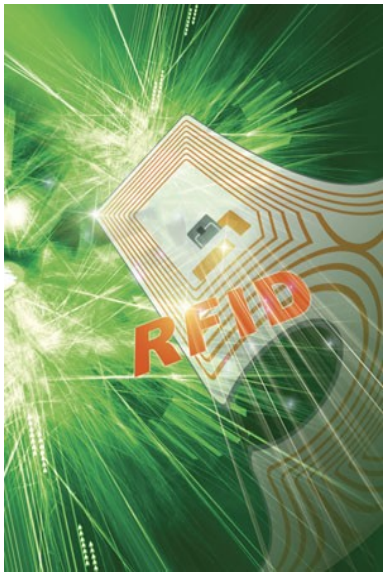
Esquema de Identificação



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

HUAB

RFID :: Identificação por Rádio Frequência



- Tecnologia para Identificar, rastrear e gerenciar pessoas e objetos sem contato e sem a necessidade de um campo visual.

- Os Sistemas de RFID são compostos por:
  - Leitor (/gravador) com antena
  - Transponder (Tag, RF Tag) (chip/antena/encapsulamento em PVC ou etiqueta)
  - Middleware (hardware + software)

RFID :: Identificação por Rádio Frequência

Vantages da Utilização da Tecnologia

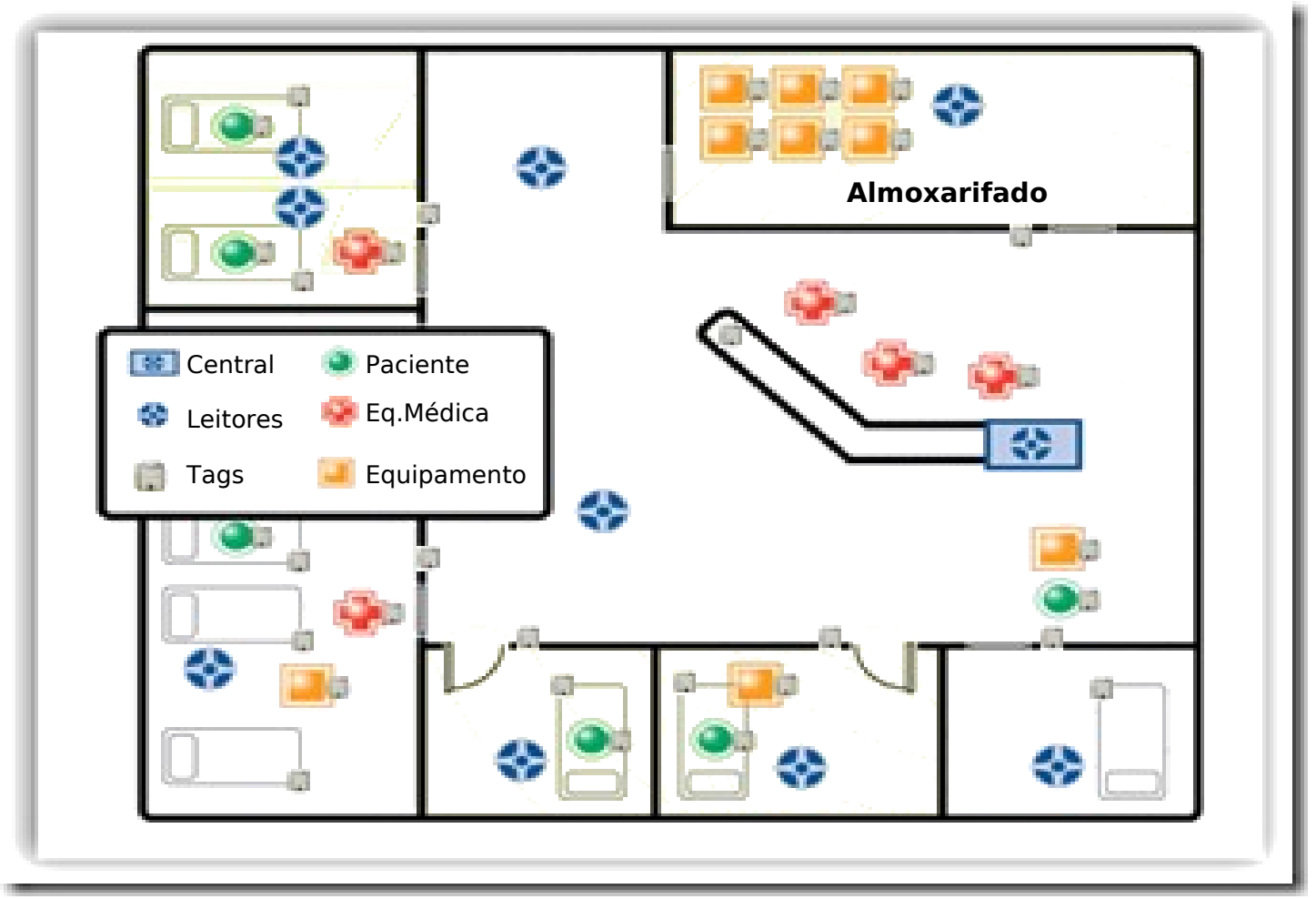
- Redução de custos operacionais;
- Eliminação de erros humanos;
- Aumento na velocidade dos processos, devido à automação dos mesmos;
- Melhor controle de qualidade com conseqüente redução de perdas;
- Operação sem a necessidade de contato físico ou permanência em ambientes insalubres (lugares úmidos, corrosivos, com extremos de temperaturas muito altas ou muito baixas), locais sujeitos à vibração, choques, etc.
- Capacidade de armazenamento dos dados coletados;
- Leitura simultânea de vários de itens;
- Captura dos dados sem necessidade de visada direta;
- Possibilidade de reutilização e alta durabilidade das etiquetas;
- Rastreabilidade de produtos e de seres vivos.

RFID e Automação Hospitalar

Automação Hospitalar

- Identificação de Pacientes (pulseiras, crachás ou microchips sob a pele):
  - Dispositivos podem armazenar registros completos que incluem desde a identidade, o tipo sangüíneo e outros detalhes da condição do paciente a fim de agilizar o seu tratamento.
  - No caso de uma emergência, o chip pode salvar vidas, já que reduz a necessidade de testes de grupo sangüíneo, alergias ou doenças crônicas, além de fornecer o histórico atualizado dos medicamentos em uso pelo paciente.
  - Com isso obtém-se maior agilidade na busca de informações e tratamento sem a necessidade de localização dos prontuários médicos.
- O uniforme dos funcionários, crachás de visitantes, remédios e equipamentos também podem ser etiquetados, criando um ambiente de administração estruturado, reduzindo erros e aumentando a segurança das pessoas.

RFID e Automação Hospitalar



Esquema de Identificação/Monitoramento

RFID :: Problemas Atuais

- **Falta de Normatização (implementações generalistas)**;
- Custo (implantação, manutenção, equipamentos, etiquetas, ...);
- **Segurança (Privacidade, Integridade, Disponibilidade, Autenticidade, ...)**

RFID :: Padronizações em Andamento

- ISO 18000-1: a ser padronizada
- ISO 18000-2: para a comunicação frequências abaixo 135 kHz
- ISO 18000-3: para uma frequência operacional em 13,56 MHz
- ISO 18000-4: para uma frequência de 2,45 GHz
- ISO 18000-6: para frequências entre 860 e 930 MHz
- ISO 18000-7: para uma operação em 433 Mhz
- ...

RFID :: Padronizações em Andamento

EPCglobal™

- Norma UHF / EPCglobal geração 2 (EPC Gen 2) criado para facilitar o uso de códigos EPC (Código Electrônico de Produto) que identificam objetos únicos (especificações técnicas de RFID e um sistema de numeração para identificação exclusiva e sem falhas)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

RFID :: Novos Termos

EPCGlobal Network Architecture

- Sistemas Abertos e/ou Fechados
  - ***Closed-loop RFID Systems***
  - ***Open-loop RFID Systems***
- Código (único) de Produto Eletrônico
  - ***EPC :: Electronic Product Code***
- Serviços de Busca/Descoberta de EPC
  - ***EPCDS :: EPC Discovery Services***
- Serviços de Informações sobre EPC
  - ***EPCIS :: EPC Information Services***
- Serviço de Nomes de Objetos
  - ***ONS :: Object Name Service***

RFID :: Características

	LF Low Frequency	HF High Frequency	UHF Ultra High Frequency	Microwave
Faixa de freqüência	30–300kHz	3–30MHz	300 MHz–3GHz	2–30 GHz
Freqüência típica de trabalho	125–134 kHz	13.56 MHz	433 MHz ou 865 – 956MHz até 2.45 GHz	2.45 GHz
Raio aproximado de alcance	menos de meio metro	Até 1,5m	433 MHz = até 100m 865-956 MHz = de 0,5m até 5m	A partir de 10m
Taxa de transferência de dados	menos de 1kbps	Aproximadamente 25 kbps	433–956 MHz = 30 kbps 2,45 GHz = 100 kbps	Até 100 kbps
Características	Curto alcance; Baixa taxa de transferência; Penetra líquidos, mas não metal	Maior alcance; Taxa de transferência razoável (equivalente a um telefone GSM); Penetra líquidos, mas não metal	Alto alcance; Alta taxa de transferência de dados; Leitura simultânea de até 100 itens; Não penetra nem líquidos nem metais	Alto alcance; Alta taxa de transferência de dados; Leitura simultânea de até 100 itens; Não penetra nem líquidos nem metais
Usos típicos	Identificação de animais	Etiquetas de preço inteligentes; Cartões de acesso/segurança	Rastreamento especial de animais; Logística	Sistema de pedágio

Projeto BRIDGE

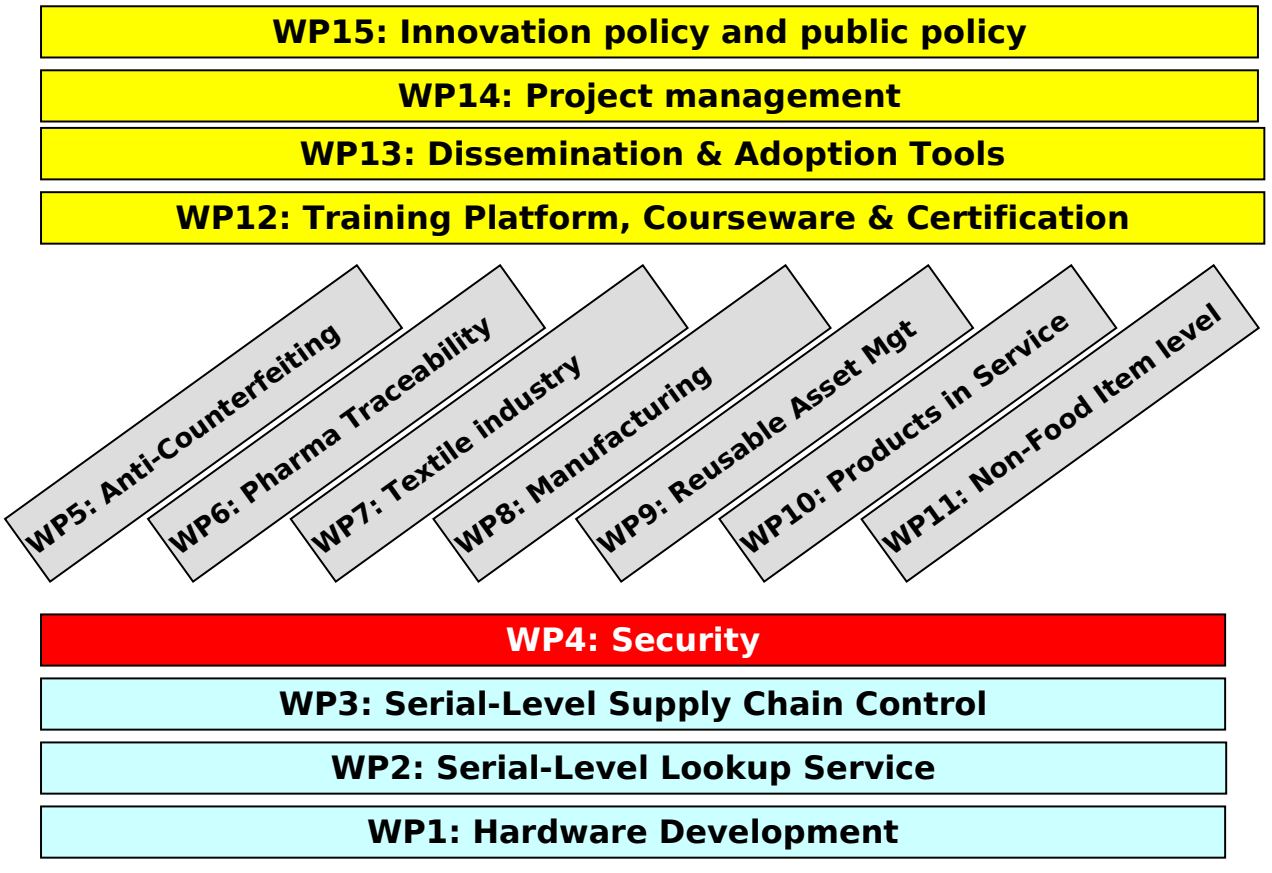
Building **R**adio Frequency **ID**entification solutions for the **G**lobal **E**nvironment

- Parcialmente financiado pela União Européia
- Principais Objetivos:
  - Desenvolver soluções para garantir a segurança da tecnologia RFID e das informações
  - Promover ações de formação acerca da tecnologia, limites e potencialidades

http://www.bridge-project.eu

Projeto BRIDGE

http://www.bridge-project.eu



WP = Pacotes de Trabalho

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Projeto BRIDGE

http://www.bridge-project.eu

WP4 :: Segurança RFID

- 3 focos principais:
  - Segurança e **Privacidade**: Análise, Requisitos e Disseminação
  - Segurança e **Integridade** de Sistemas RFID
  - Segurança na **Infraestrutura de Redes** RFID

Tag Security
RFID Trusted Network
Anti-Cloning
Network Confidentiality
Data Integrity

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Papers RFID / BRIDGE (WP4 :: Security)

http://www.bridge-project.eu

- BRIDGE WP4 :: Security Analysis Report
- BRIDGE WP4 :: Anti Clone Prototype
- BRIDGE WP4 :: Anti Clonning Demonstrator
- BRIDGE WP4 :: Economic Relevance Secure RFID Solutions
- BRIDGE WP4 :: Interim Security Deliverable
- BRIDGE WP4 :: RFID Network Confidentiality
- BRIDGE WP4 :: Secure Semi-passive RFID Tags
- BRIDGE WP4 :: Security Technology Roadmap
- BRIDGE WP4 :: Supply Chain Integrity
- BRIDGE WP4 :: Tag Security
- BRIDGE WP4 :: Threat Model Analysis
- BRIDGE WP4 :: Trusted Business Interaction
- BRIDGE WP4 :: Trusted Reader Authentication
- BRIDGE WP4 :: Design Trusted Reader
- BRIDGE WP4 :: Final Report Network Confidentiality
- BRIDGE WP4 :: Trusted Reader Hardware Description

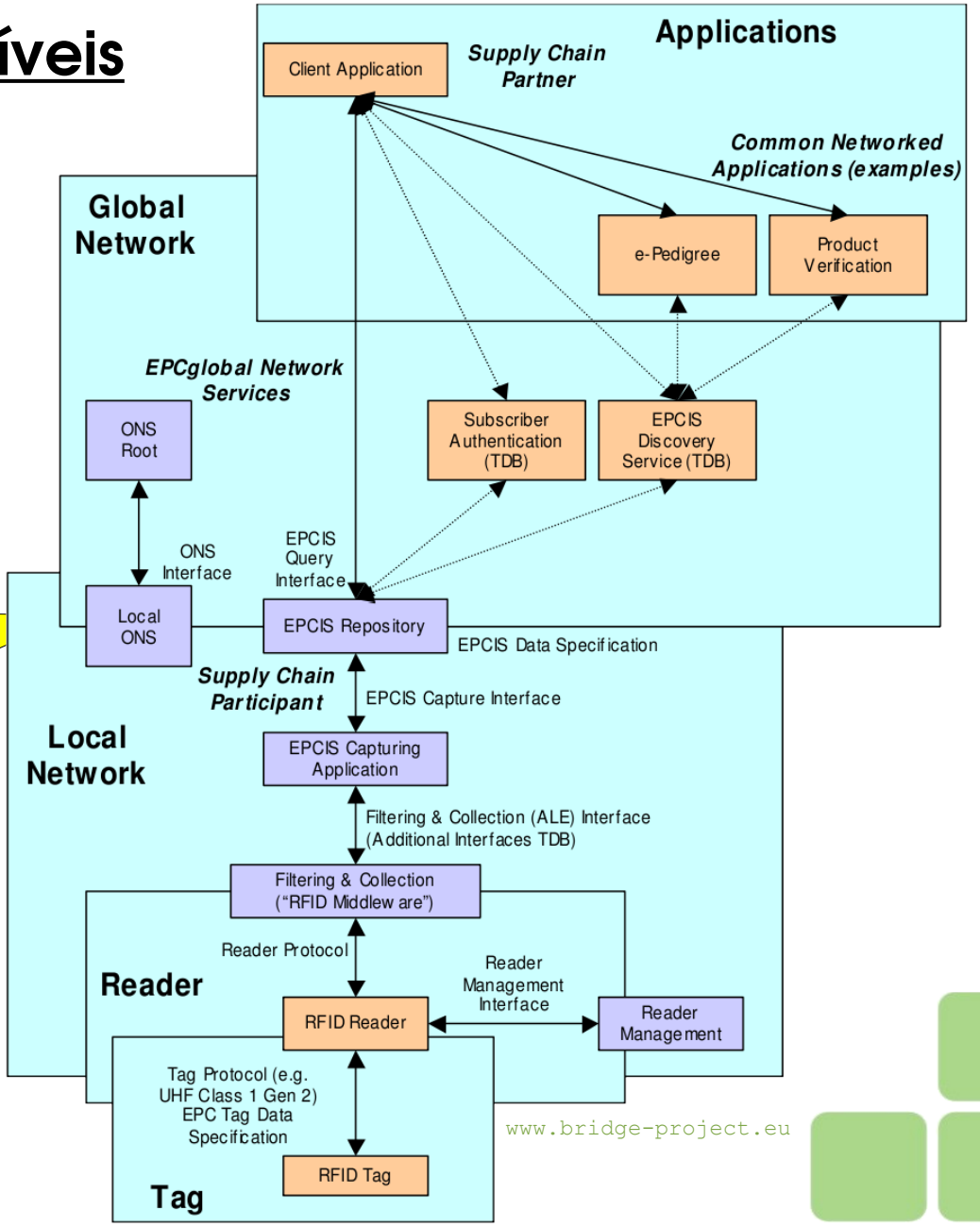
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

RFID :: Novos Problemas de Segurança

Abordagem em 4 Níveis

- *Tags*
- *Leitores (readers)*
- *Rede(s)*
- *Aplicações*

34 (trinta e quatro) novos problemas relatados no WP4/BRIDGE



www.bridge-project.eu

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

RFID :: Novos Problemas de Segurança

Tags RFID

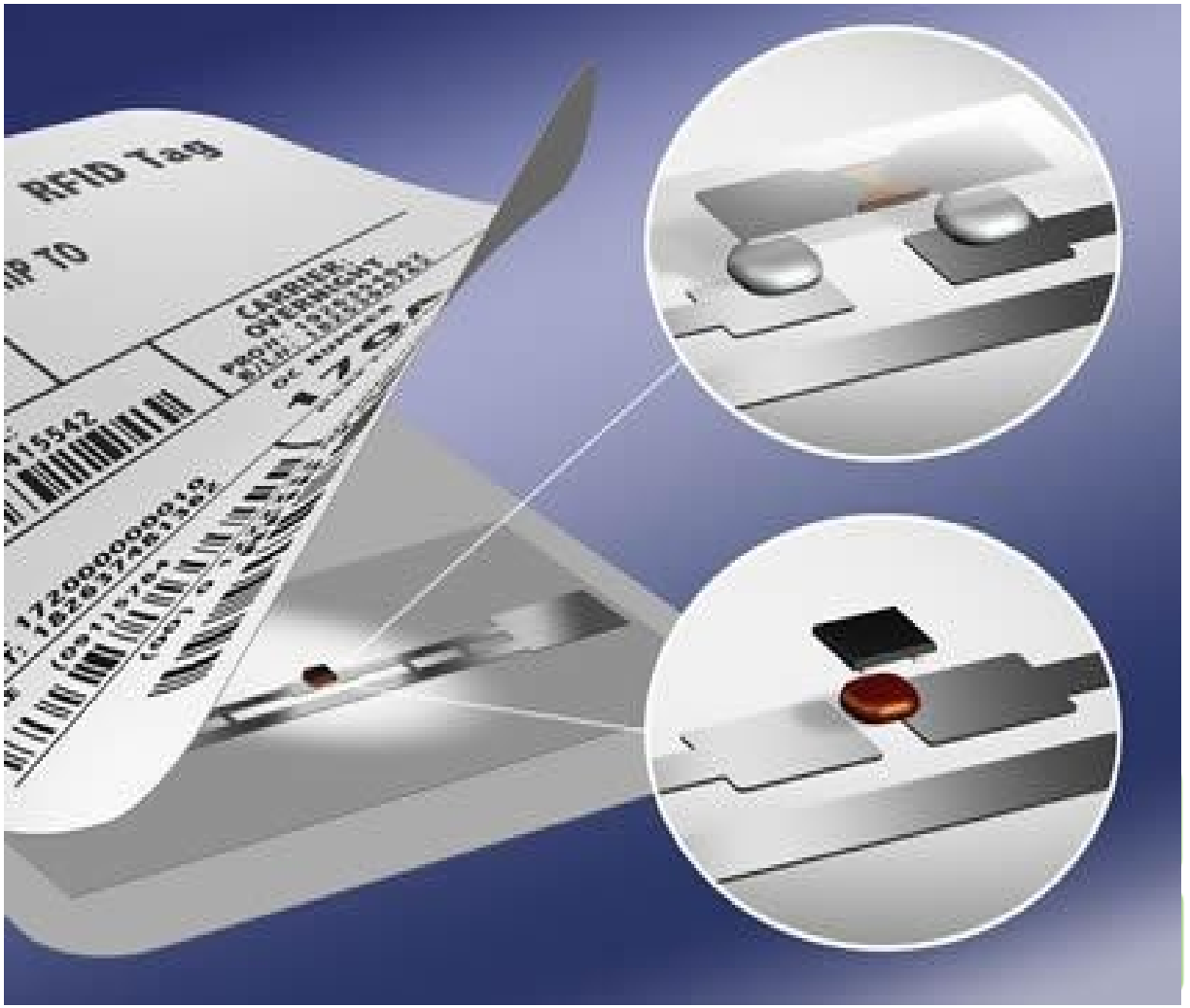
- *Extravio/troca (intencional ou não) de tags*
  - *Uso de sistemas de monitoramento integrado (com alertas de incidentes)*
  - *Incidência possível, porém menor que em procedimentos tradicionais de identificação*
  - *Foco na padronização e checagem de procedimentos com interferência humana.*
  - *Dependência (mesmo que parcial) de pessoas (processos não-automatizados)*
  - *Custo*

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

RFID :: Novos Problemas de Segurança

Tags RFID

- *Clonagem de tags*
  - *Autenticação (criptografia)*
  - *Tags Passivas/Ativas*
  - *Tamanho (capacidade de armazenamento)*
  - *Suporte nas tags e leitores*
  - *Custo*



RFID :: Novos Problemas de Segurança

Tags RFID

- *Garantia de (in)disponibilidade de Informações após uso final*
  - *Política de uso (desabilitar/inutilizar/retirar) tag após fim da necessidade de indentificação*

RFID :: Novos Problemas de Segurança

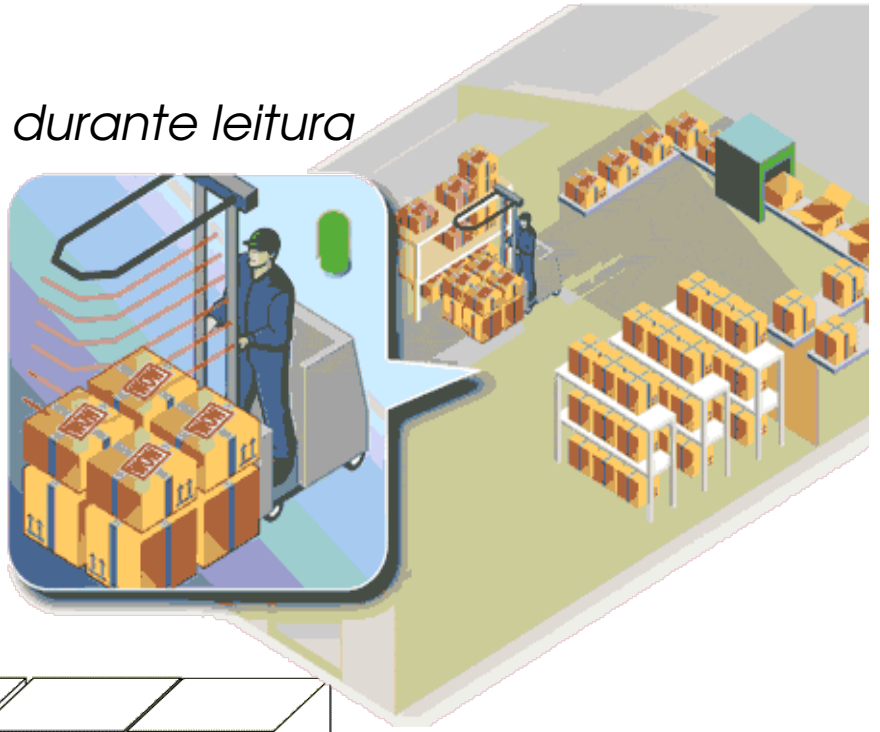
Tags e Leitores RFID

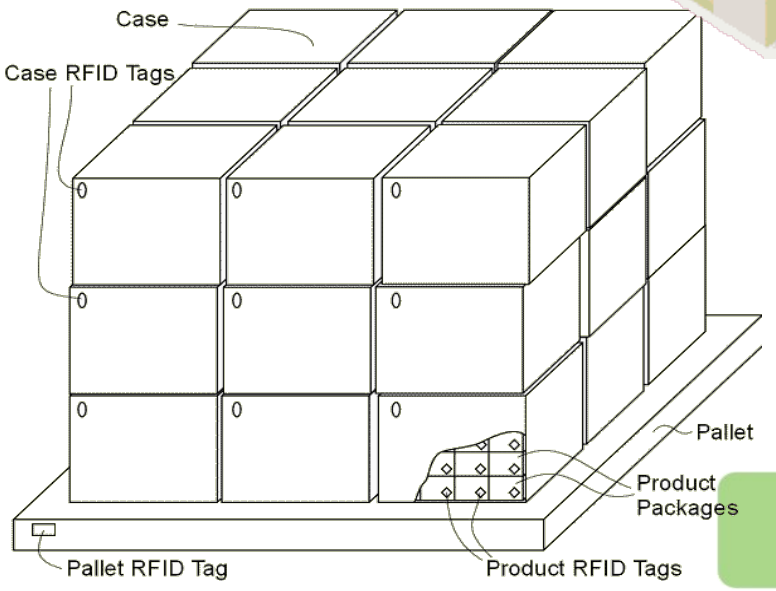
- *Disponibilização de Informações (leitura indevida de informações das tags)*
  - *Autenticação (criptografia)*
  - *Tags multiperfis (limitação de acesso anônimo)*
  - *Tags Passivas/Ativas*
  - *Tamanho (capacidade de armazenamento)*
  - *Suporte nas tags e leitores*
  - *Custo*

RFID :: Novos Problemas de Segurança

Tags e Leitores RFID

- *Garantia de disponibilidade de Informações durante leitura*
  - *Uso de padrão de frequência adequado (permissão de múltiplas leituras simultâneas)*
  - *Uso de tags individuais e coletivas*
  - *Controle integrado à aplicação (quantitativo de tags e alertas de ausência de dados)*
  - *Custo*





RFID :: Novos Problemas de Segurança

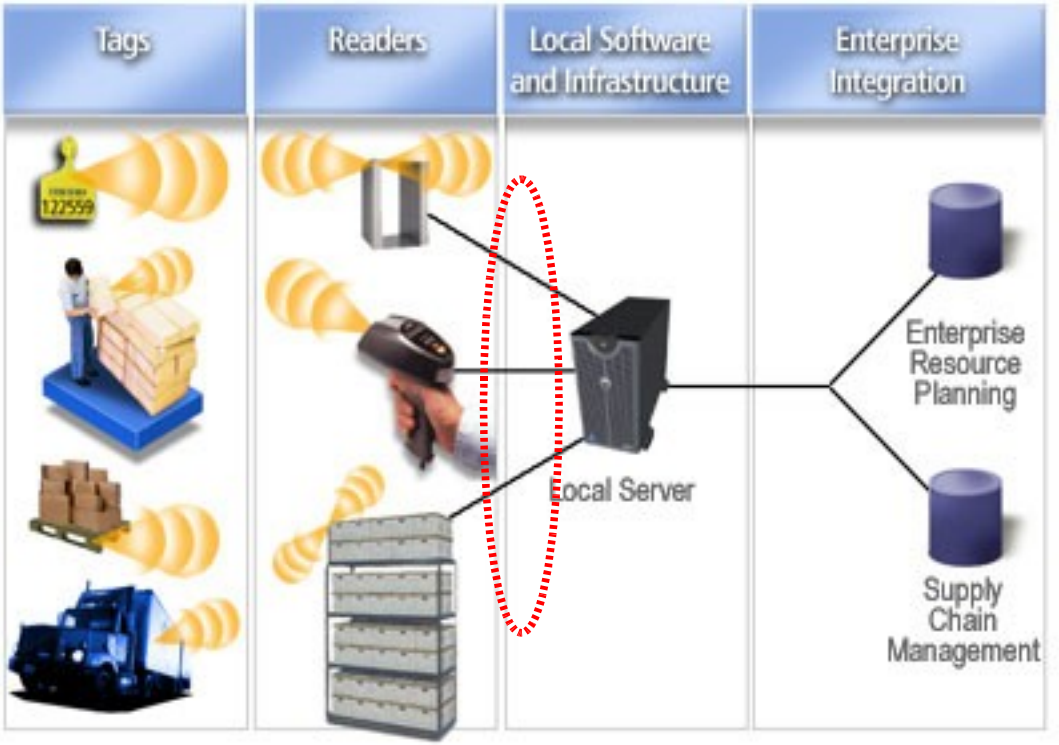
Tags e Leitores RFID

- *Controle/bloqueio/histórico de acessos indevidos (injeção não autorizada de dados em tags de informações falsas e/ou não padronizadas)*
  - *Autenticação de leitores*
  - *Integração de leitores com sistemas de registro (logs)*
  - *Vistoria periódica nas tags (comparação/conferência com padrões e histórico)*
  - *Tags não comunicam-se diretamente com sistemas (somente com leitores)*
  - *Tags não podem impedir a inserção de dados por leitores (autenticados !?)*

RFID :: Novos Problemas de Segurança

Leitores RFID x Redes x Aplicações

- *Controle do tráfego de Informações entre Leitores e Aplicações*
  - *Autenticação de leitores (no acesso às aplicações)*
  - *Garantia de integridade e confidencialidade na rede (criptografia)*
  - *Soluções caminham para padrões abertos e consolidados em aplicações tradicionais*



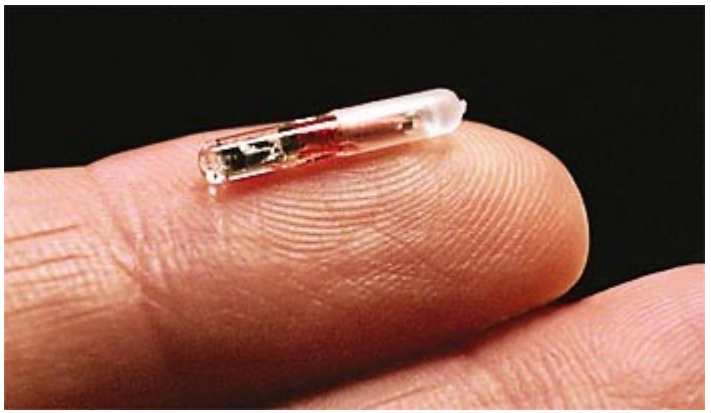
RFID :: Novos Problemas de Segurança

Outras preocupações à vista

- *Política hierárquica (perfis) de acesso a informações de pacientes (o que pode ser acessado? por quem pode ser acessado? quando pode ser acessado?)*
- *Ataques de negação de serviço (Denial of Service) contra infra-estrutura de comunicação (rede) e/ou leitores (injeção proposital e em grande quantidade de dados falsos)*
- *Poluição espectral (faixas de frequência de sistemas fechados e abertos)*
- *Disseminação de worms/vírus por tags/leitores (alterando/apagando tags)*
- *Nível de automatização de controle de acesso a ambientes críticos (Acessos indevidos x Bloqueio de acesso por falha)*
- *Integração com sistemas externos: farmácias, laboratórios, rede bancária, redes de crédito, funerárias (!!??)*

Polêmica :: Implantes RFID

VERICHIP



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Polêmica :: Implantes RFID

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

no verichip inside ®

Polêmica :: Implantes RFID

Polêmica :: Implantes RFID

Código de Barras ≠ RFID ≠ GPS

RFID + GPS = Mito (!?)

- Até quando?
  - Limitações Atuais = tamanho (GPS) e necessidade de bateria de longa duração
- Solução (ideal !?) para Identificação / Monitoramento
  - Privacidade !!??
- Vídeo Verichip / Baja Beach Club

Referências Bibliográficas Complementares

• KOBAYASHI, L., FURUIE, S. **"Security in Medical Information"**, In: Revista Brasileira de Engenharia Biomédica, v.23, n.1, p. 53-77, apr 2007.

• HAMILTON, D.L., **"Identification and evaluation of the security requirements in medical applications"**, In: Proceedings of the 5th Annual IEEE Symposium on Computer-Based Medical Systems, Durham, p. 129-137, 14-17 jun 1992.

• VAN DER HAAK, M., WOLFF, **"Data security and protection in cross-institutional electronic patient records"**, International Journal of Medical Informatics, v. 70, n. 2-3, p. 117-130. 2003.

• BUNBAK, M., **"Analysis of potential RFID security problems in supply chains and ways to avoid them"**, Rotterdan Business School, mai 2005.

• BONO, S., **"Security Analysis of a Cryptographically-Enabled RFID Device"** 14th USENIX Security Symp, p. 1-15, 2005.

• FELDHOFER, M., DOMINIKUS, S., **"Strong Authentication for RFID Systems Using the AES Algorithm"** Cryptographic Hardware and Embedded Systems (CHES 2004), p. 357-370, 2004.

• JUELS, A. **"Minimalist Cryptography for Low-Cost RFID Tags"** 4th InternationalConference in Security in Communication Networks, p. 149-164, 2004.

Links Relacionados

- EPC Global
  - http://www.epcglobalinc.org
- Projeto BRIDGE
  - http://www.bridge-project.eu
- RFIDSec :: Workshop on RFID Security
  - http://www.rfid-sec.org
- Blog RFID Technology
  - http://rfidtek.blogspot.com
- Blog RFID Business
  - http://rfidbusiness.blogspot.com
- Rieback, R. M. et al. Is Your Cat Infected with a Computer Virus?
  - http://www.rfidvirus.org/papers/percom.06.pdf

Perguntas