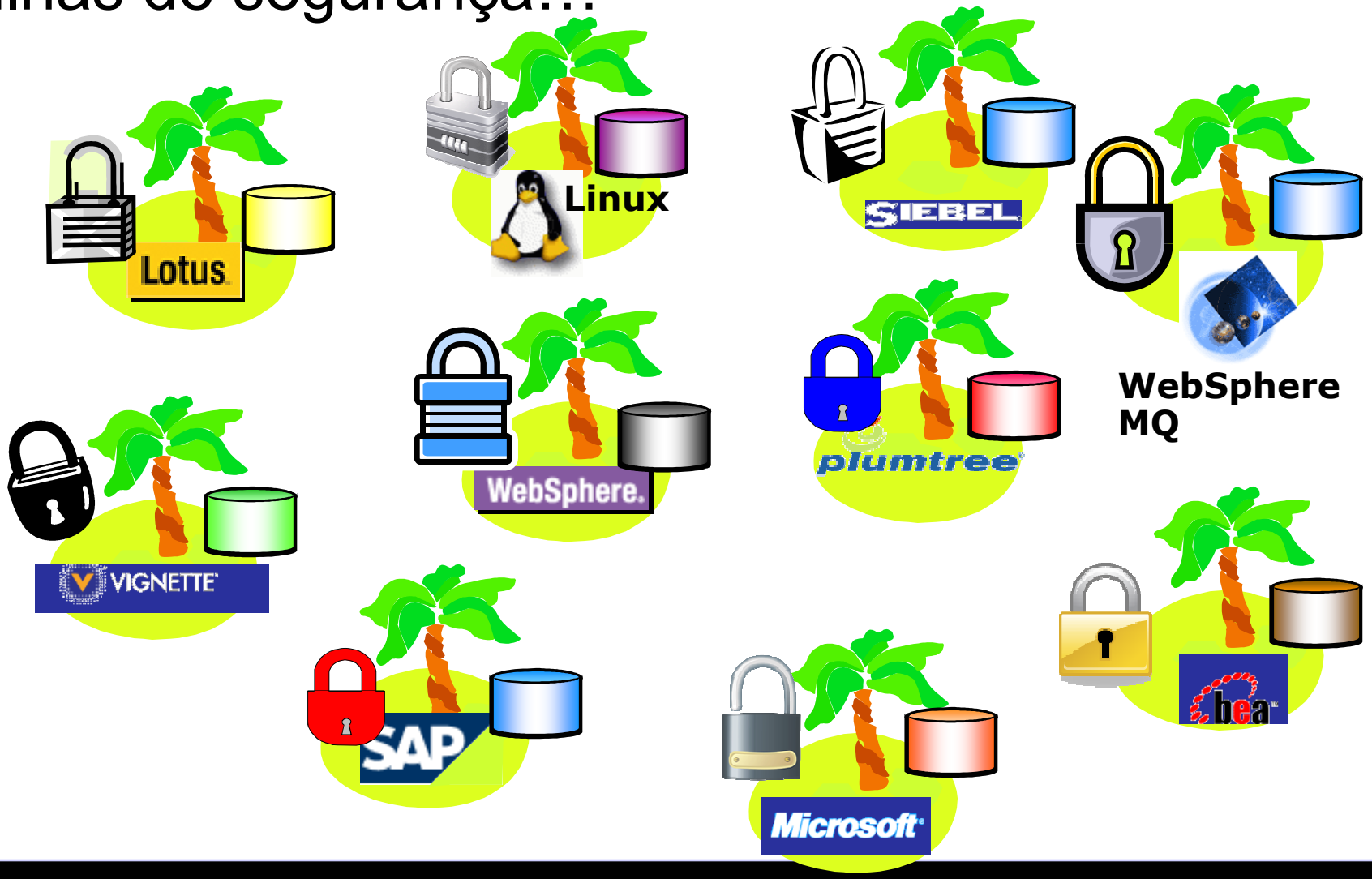
IBM Security Forum

Soluções para um ambiente seguro

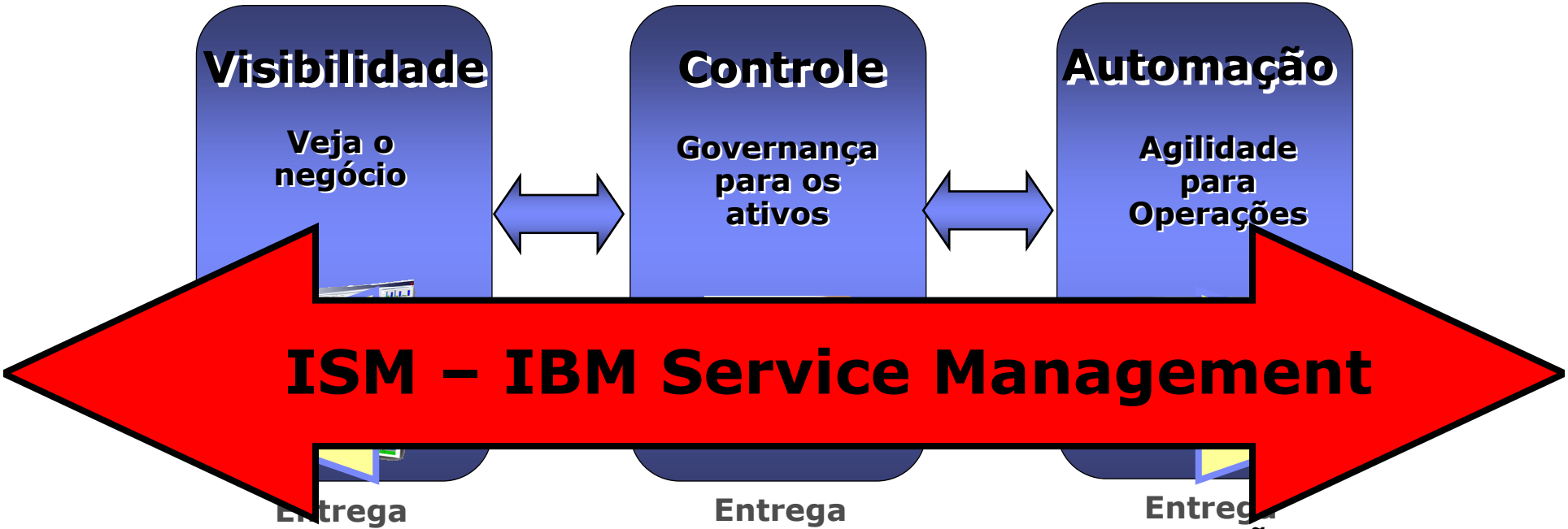
Os 4 A's do IAM e o Pre-Crime

Henrique Bernardes, CISM, CISSP
Tivoli Security Sales Manager
Bernardes@br.ibm.com

As ilhas de segurança…



Resposta para as ilhas de segurança = **ISM**

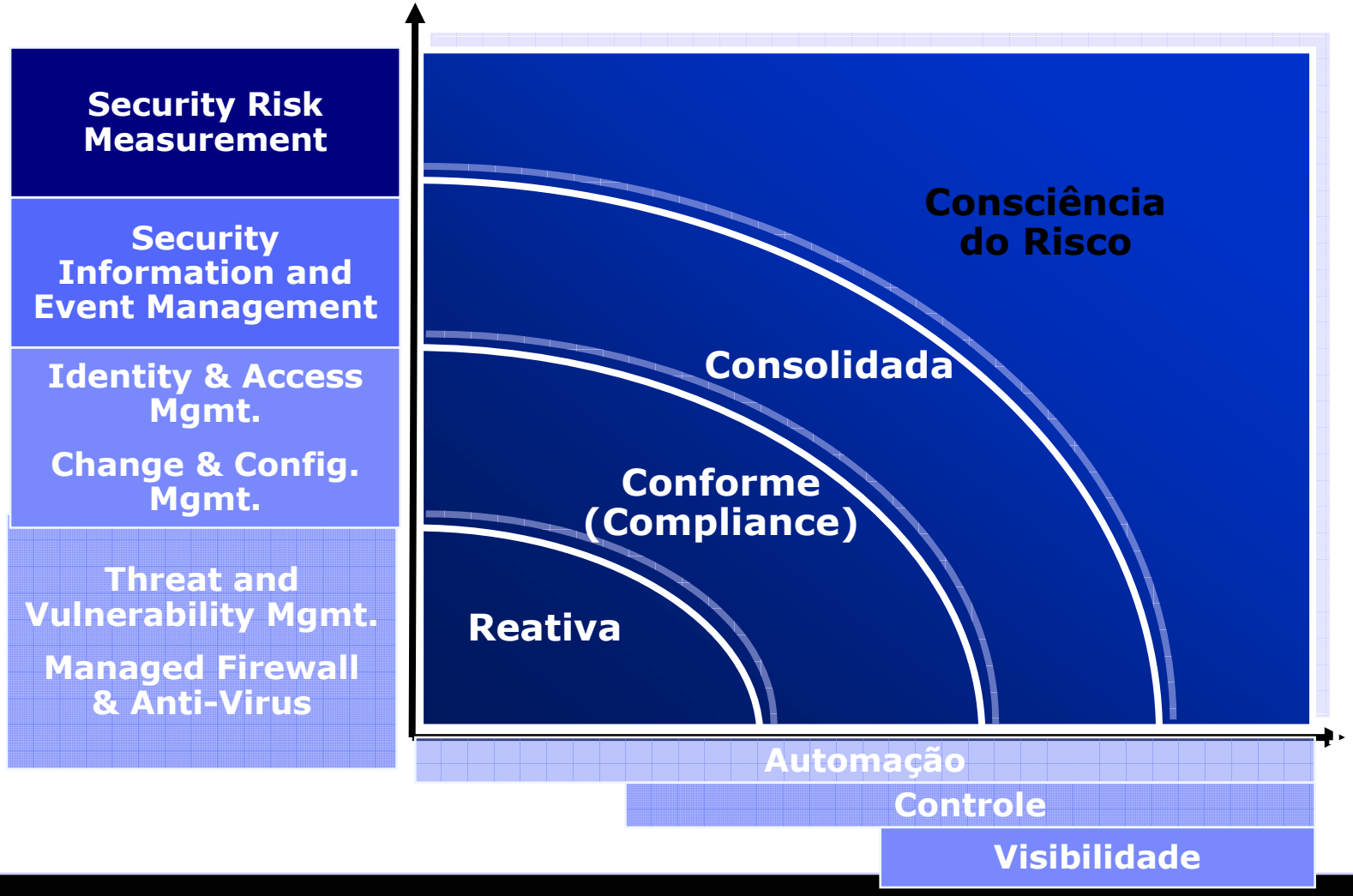


- Console de Operação de Segurança (SOC)
- Dashboard de Compliance

- Controle de acessos, baseado em politicas, dentro e fora das bordas
- IDs sincronizados

- Usuários provisionados via Workflow
- Sign-On automático

ISM – De reativa a consciente



O que é “RISCO”?

- Risco: Qualquer coisa que possa impedir o atingimento de objetivos.

Risco Externo
- Weather
- Political changes
- Regulatory changes

Risco de Mercado
- Competitive events
- Pricing
- Technology advances

Risco Operacional
- Secure access to databases, applications
- Protection of all systems and resources
- Manage and remediate system vulnerabilities

Risco de Crédito
- Default of borrower
- Maintenance of credit rating
- Outsourcing
- Cost of money

Risco operacional está relacionado com a operação com sucesso dos processos de negócio, e é o risco mais controlável.
SEGURANÇA é o elemento mais importante do Risco Operacional.

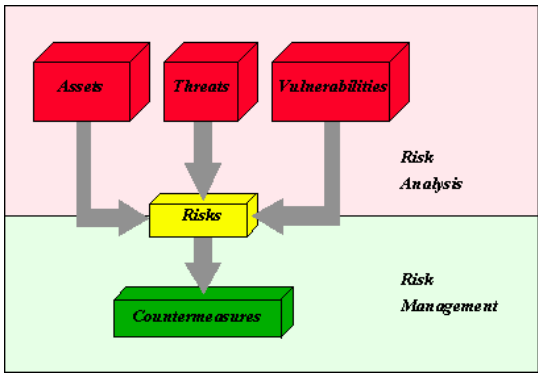
Gestão de Risco contra a FRAUDE

A OPORTUNIDADE: elemento fundamental no esquema da fraude

- OBJETIVO:
  - Eliminar a percepção de oportunidades
  - Reduzir o risco a níveis aceitáveis

1. Contramedidas/Controles Internos
   - Preventivos e Detectivos
2. Procedimentos de detecção da FRAUDE
3. Investigação de possíveis FRAUDES

Fonte: José Claudio Treviño – Gerente Investigación de Fraude E&Y Monterrey



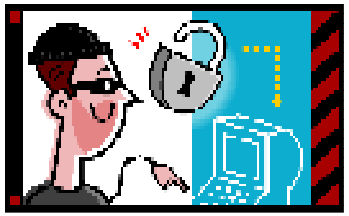
Source: CRAMM (CCTA Risk Analysis Management and Methods)

Controles para Gestão do RISCO

- O controle de perímetro “Detectivo” é apenas um dos vários desafios da Gestão de Riscos de TI

Além do Risco tradicional, outros desafios…

- Riscos de TI
  - **Roubo de informações** confidenciais
  - Forçar a utilização de **políticas de segurança**
  - Privilégios redundantes e **brechas de segurança**
  - **Trilhar utilização** dos acessos
  - **Proteger ativos** críticos
  - **Conflito de interesses**



- Despesas Operacionais
  - **Gerenciamento descentralizado** de identidades de usuários e políticas de acesso
  - Dificuldade em filtrar, priorizar, correlacionar e atuar na **resolução eventos de segurança**
  - Como **delegar a administração de usuários** de forma segura?
  - **Vários pontos de autenticação** necessários por usuário
  - Demandas e requisições de usuários sempre necessitam do **envolvimeto de várias áreas** na resolução
  - Criação e remoção de contas e provilégios de forma manual, com **fluxos de aprovação também manuais e despadronizados**

- Compliance
  - Processos manuais na gestão de identidades **dificultam a rastreabilidade** pela auditoria
  - **Controles descentralizados** de acessos
  - Políticas de **senhas inflexíveis** e falta de mecanismos mais fortes de autenticação
  - **Dificuldade no deprovisionamento instantâneo** de acessos e contas de usuários
  - Dificuldade na identificação e **remoção de contas inativas**
  - Dificuldades na **segregação de funções** e papéis conflitantes
  - **Auditoria de eventos** de segurança descentralizada e incompleta

- E ainda…
  - Equilibrar o dilema do nível de proteção dos ativos e a necessidade de geração de novos negócios
  - Estreitar o relacionamento com os clientes atuais

O que CIOs, CSOs e CFOs estão nos dizendo…

- Aumento na complexidade para compliance
  "É muito trabalhoso garantir que todas as regulamentações estão sendo endereçadas. E ai tudo precisa ser feito novamente no ano seguinte."
- Sobrecarga no Help Desk
  "25% dos chamados do help desk são relacionados ao reset de senhas esquecidas!"
- Custos de administração crescentes
  "Não existe mais orçamento para contratação de mais administradores de TI, mas nossa população de usuários esta crescendo, principalmente na medida em que colocamos mais clientes/parceiros online."
- Contas Fantasma
  "Continuam existindo contas de usuários que saíram da empresa ha muito tempo!"
- Privilégios acumulados e inapropriados
  "Empregados e parceiros ao mudarem de responsabilidade continuam adquirindo novos privilégios de sistemas, e nenhum é removido. Como corrigir isso?"
- Requisitos de Auditores
  "Auditoria interna e externa necessitam saber que existem controles suficientes sobre os sistemas de TI e acessos a dados privados. Auditores de forma geral não se preocupam com quanto isso custaria."

SEGURANÇA

Cinco maneiras de proteger a sua empresa de ex-funcionários

Framingham - Demissões em massa podem gerar comportamento destrutivo. Conheça os passos necessários para proteger a sua empresa desse tipo de reação hostil.

Por **COMPUTERWORLD/EUA**
24 de março de 2009 - 07h00

Um alto executivo deixa a empresa e leva com as fotos de família, a sua caneta de estimação e, também, as senhas de centenas de funcionários.

RECURSOS:
Imprimir Texto
Enviar por e-mail
Comentar

A analista da IDC aconselha também que seja instalada a infraestutura de IAM – gestão de identidade e acesso, da sigla em inglês. "[o sistema] Controla quem, o que, quando e onde das atividades dos usuários," explica Hudson. Ter a habilidade de monitorar e avaliar os acessos é fator crítico para atender regulamentações governamentais e identificar mau uso do sistema.

CONTEÚDO RELACIONADO

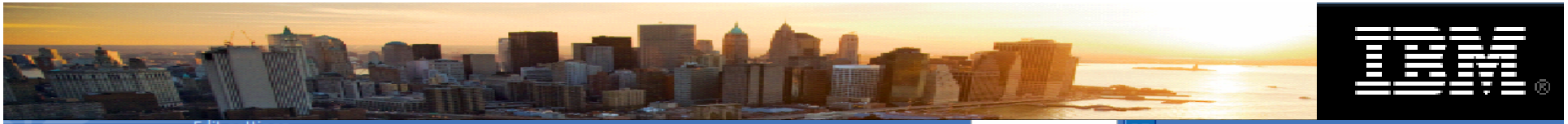
- Nokia anuncia demissão de 1,7 mil empregados
- SAP inicia plano de demissões sem revelar número de dispensados
- Dell anuncia novas demissões de funcionários no mundo inteiro

Dicas de segurança para os bons e maus momentos
Independente da condição econômica, a IDC recomenda que estes passos sejam seguidos para evitar perda de dados após a saída de funcionários:

* Documente cada acesso dos funcionários na rede, aplicações, servidores e ao prédio da empresa.
* Feche os acessos remotos.
* Invalide nomes de usuários e senhas.
* Se o funcionário trabalhou em TI, modifique o root access e acesso a rede.
* Acabe com o acesso externo ao sistema de telefone.
* Garanta que os smartphones e celulares sejam devolvidos juntos com os laptops.
* Use software de monitoramento para analisar o tráfego de rede.

ÚLTIMAS NOTÍCIAS

- Malware sequestra arquivos de internautas e pede resgate em dinheiro
- Falha de segurança no Firefox deve ser corrigida na próxima semana
- Empresas temem roubo de dados por conta da crise, diz KPMG
- Banese elimina 2,4 milhões de spams por mês com ferramenta de bloqueio
- Cinco maneiras de proteger a sua empresa de ex-funcionários
- HP lança ferramenta gratuita para medir desenvolvimento seguro em Flash
- Bug novo descoberto no Twitter pode ser usado para ataque em massa



Edit settings

Search w3 GO

IBM

w3 BluePages

w3 Home | BluePages | HelpNow | Feedback

BluePages home

My profile

My Blu...

Edit settings

Help

My BluePages lists

Create lists of profiles you view often.

To get ...

Add ...

links on t...

page and when ...

an employee's profile.

Updated on 29 Oct 2008

BlueMessages: BluePages Survey: We always value your fe... k. Tell us how we are responding to your needs. Next >

You have an unpublished draft dated 29 Oct 2008

My profile

Edit my profile | BluePages wizard

Search contact inf... ice profil...

Se...

Name

...BILE

My preferred ... method is e-m...

Phone: 55-11-9496-6...

E-mail: bernardes@br.ibm...

Notes mail: Henrique Bernardes ...eixeira/Brazil/IBM@IBMBR

Sametime status: • Teixeira, Henriqu... ...des Batista | Sign out

...eando

...eixeira, Henrique ...rdes Batista

...ort to chain

...nager

• Exter... relationship...

DOWNLOAD GRÁTIS:

www.ibm.com/software/tivoli/resource-center/security/code-directory-server.jsp

Conceito IAM “Identity and Access Management”
Gestão de Identidades e Acessos

*"Identity and Access Management (**IAM**) é um sistema integrado de:*

processos de negócio, políticas, práticas e tecnologias

que habilita as organizações a controlar o
***acesso dos usuários às aplicações e recursos críticos**,*
protegendo informações confidenciais de usuários não autorizados.”

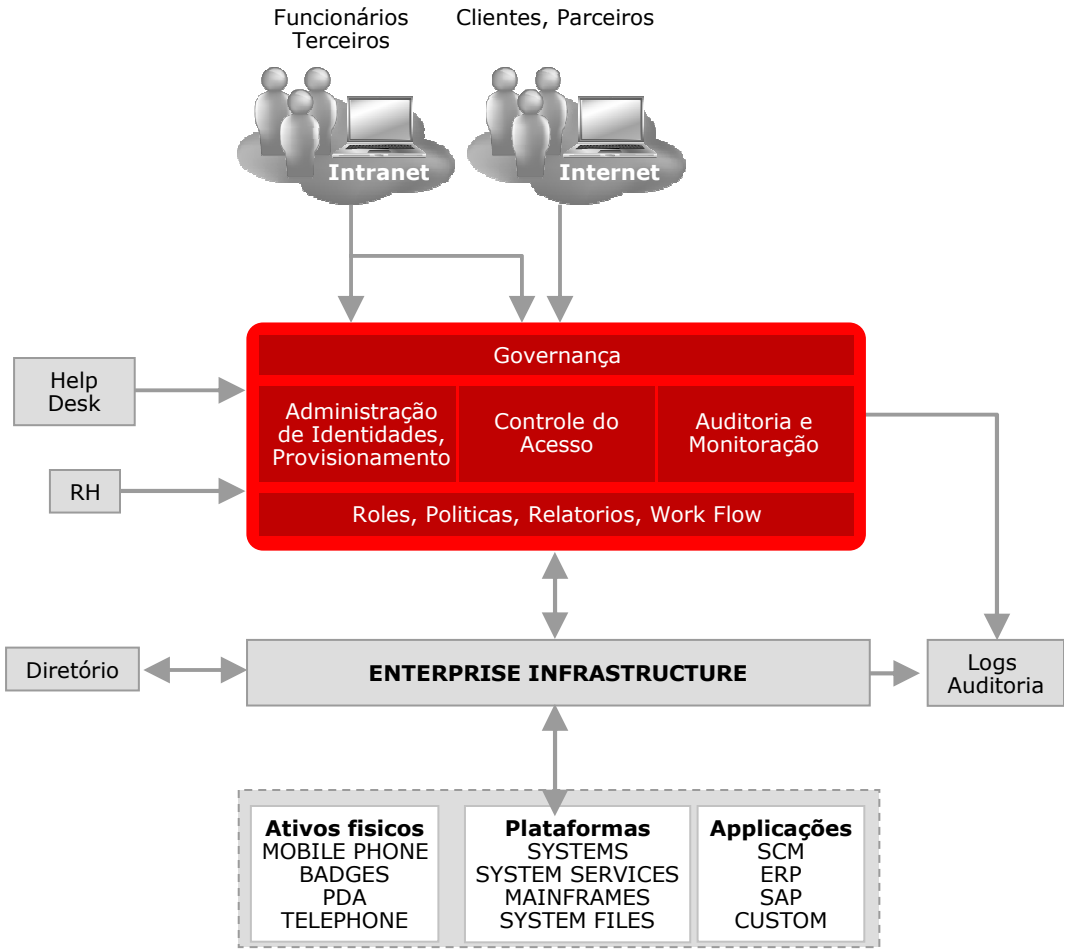
A plataforma “PRE-CRIME”

- **Previnir**
- **Detectar**
- **Corrigir**

Conceito IAM “Identity and Access Management”
Gestão de Identidades e Acessos

- Qualquer identidade (funcionários, terceiros, parceiros, clientes)
- Todos os pontos de *enforcement*
- Suite única, **modular e integrada**
- Baseada em padrões
- Utilizando melhores práticas

- **Administração**
  - Gerenciamento de Identidade automatiza a administração, gerenciamento do cliclo de vida das identidades e seus relacionamento na Organização
- **“Enforcement”**
  - Gerenciamento de Acesso provê o reforço das políticas e regras da organização
- **Auditoria**
  - Evidência forte dos controles de segurança



Gestão de Identidades e Acessos - IAM

Gestão de Identidades e Acessos

Identity Administration	Access Management	Monitoring and Auditing
Quem é você?	**O que você pode fazer?**	**O que você fez?**
A: **Administração**	A: **Autenticação** A: **Autorização**	A: **Auditoria**

OS 4 A's da SEGURANÇA

IAM – Gestão de Identidades e Acessos

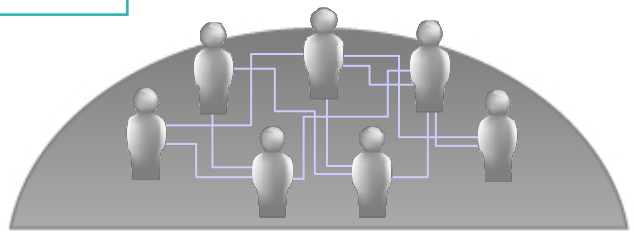
Disciplina	Abordagem de Mercado
Gestão de Identidades e Provisionamento	PASSWORD MANAGEMENT PROVISIONING ID ADMINISTRATION META DIRECTORY DIRECTORY MAINFRAME
Controle de Acessos	FEDERATION, FEDERATED SSO WEB SERVICES, SOA WEBSITES, WEB SSO ENTERPRISE SSO OPERATING SYSTEMS APPLICATIONS
Auditoria, Monitoração e Governança	MONITORAÇÃO EVENTOS AUDIT COMPLIANCE GOVERNANÇA MAINFRAME

O desafio da Gestão de Identidades e Acessos

> A operação de concessão de acessos realizada de forma descentralizada, e dificultada pelo volume de milhares de solicitações/mês

> Dificuldade em gerenciar acessos

> Custos altos na operação

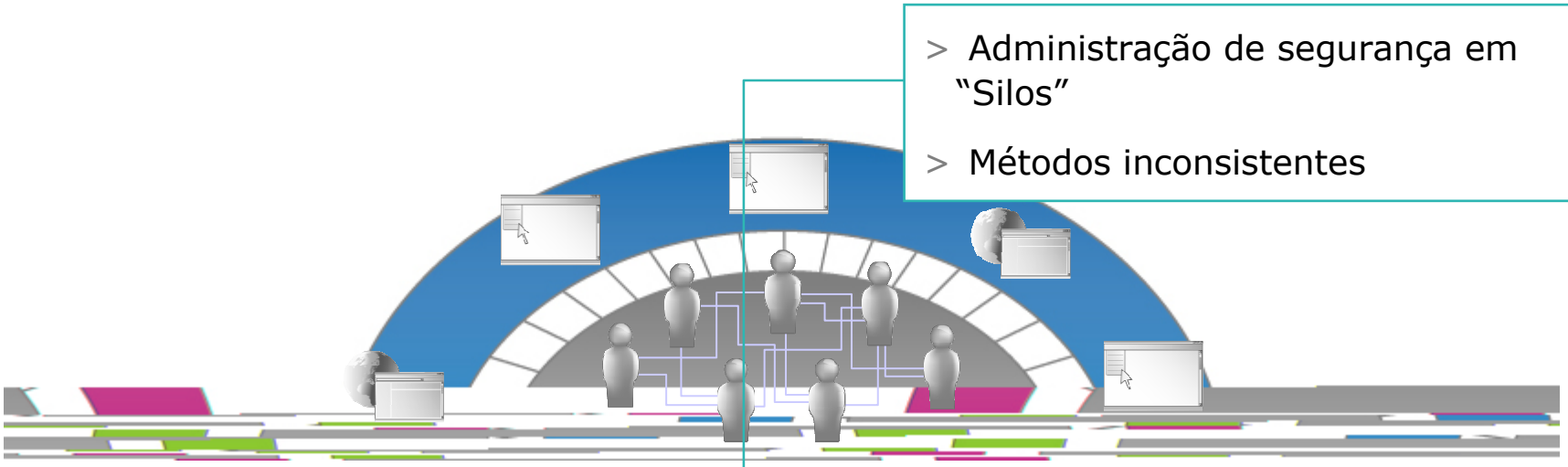


MUITOS USUÁRIOS

>Funcionarios

>Terceiros

O desafio da Gestão de Identidades e Acessos



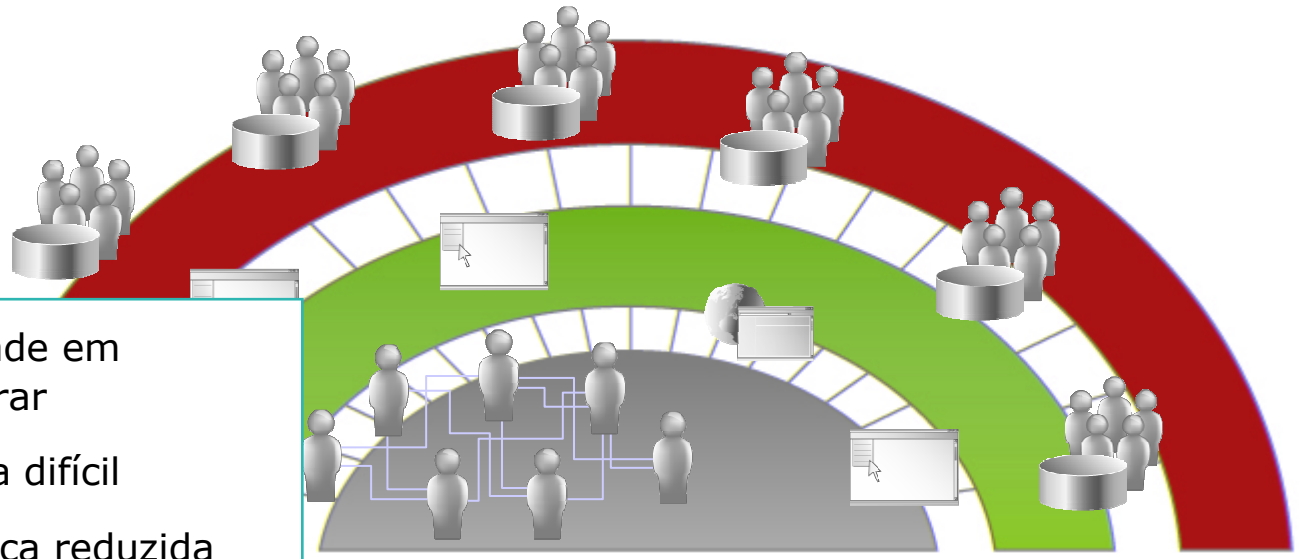
> Administração de segurança em "Silos"

> Métodos inconsistentes

MUITOS USUÁRIOS
>Funcionarios
>Terceiros

MUITAS APLICAÇÕES
>Financeiras
>Produção
>Mesa de operação
>ERP
>CRM

O desafio da Gestão de Identidades e Acessos



- Dificuldade em Administrar
- Auditoria difícil
- Segurança reduzida

MUITAS IDENTIDADES
>Mainframe
>Banco de Dados
>AD
>LDAP
>ERP…

MUITOS USUÁRIOS
>Funcionarios
>Terceiros

MUITAS APLICAÇÕES
>Financeiras
>Produção
>Mesa de operação
>ERP
>CRM

O desafio da Gestão de Identidades e Acessos

MUITAS IDENTIDADES
>Mainframe
>Banco de Dados
>AD
>LDAP
>ERP…

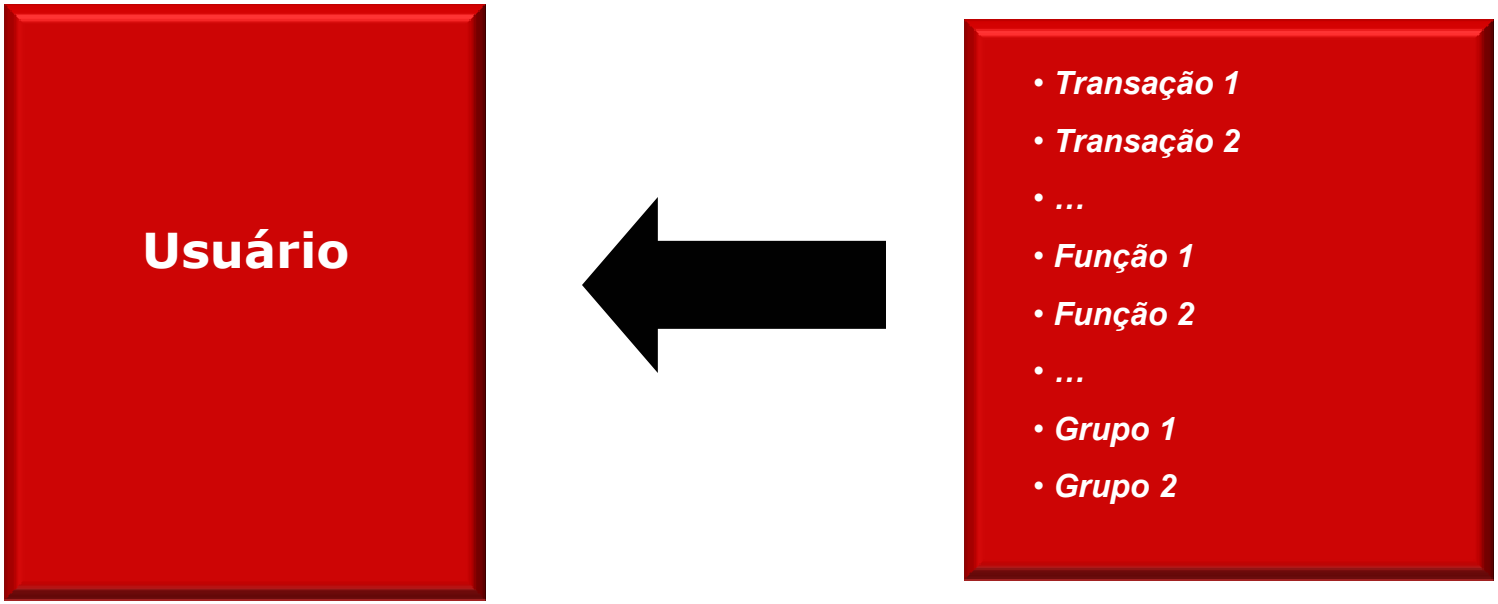
MUITOS USUÁRIOS
>Funcionarios
>Terceiros

MUITAS APLICAÇÕES
>Financeiras
>Produção
>Mesa de operação
>ERP
>CRM

MUITAS ILHAS
>Muitas questões táticas
>Gerenciar usuários, senhas, etc.

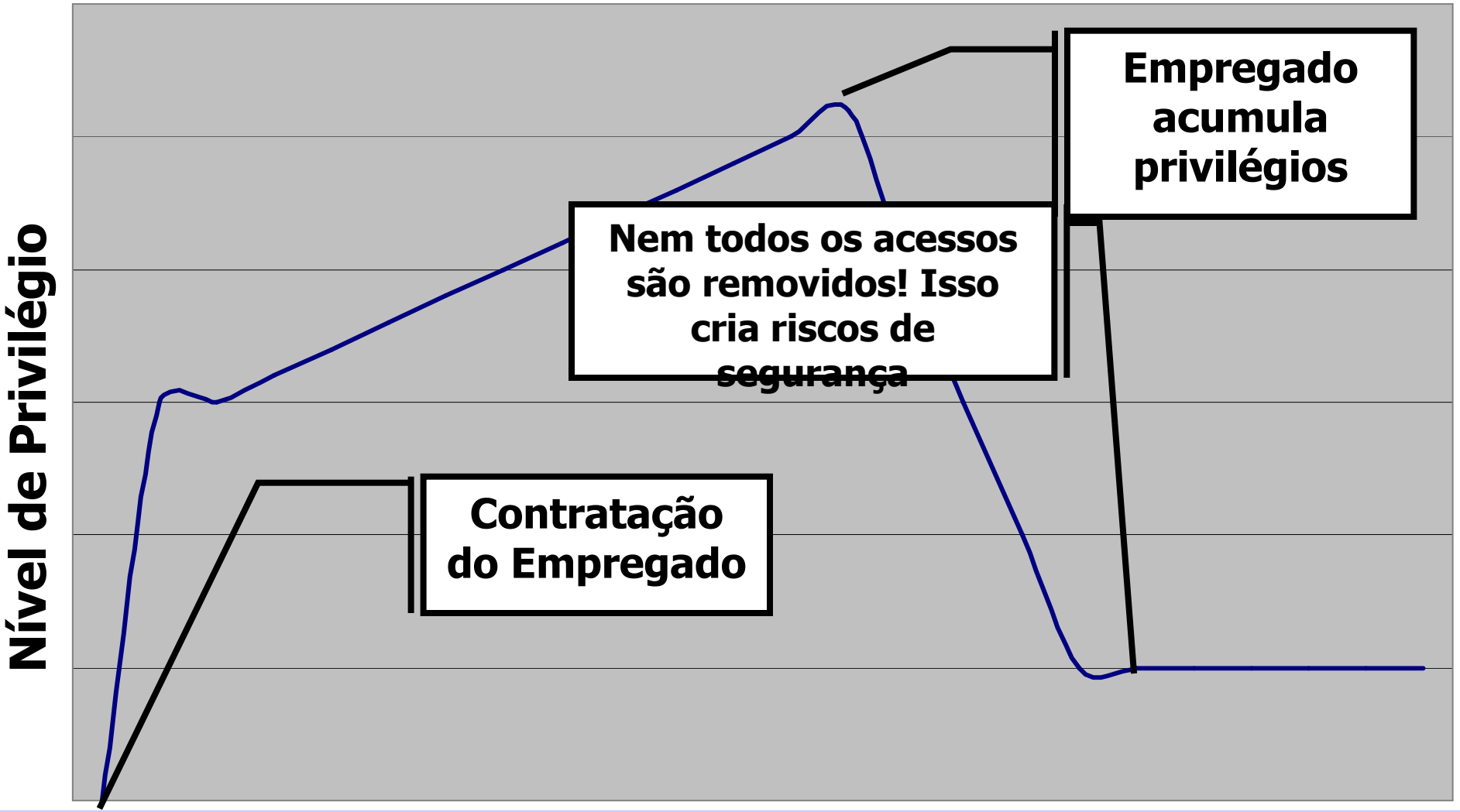
Modelo Usual de Concessão de Acesso

DAC: Discretionary Access Control

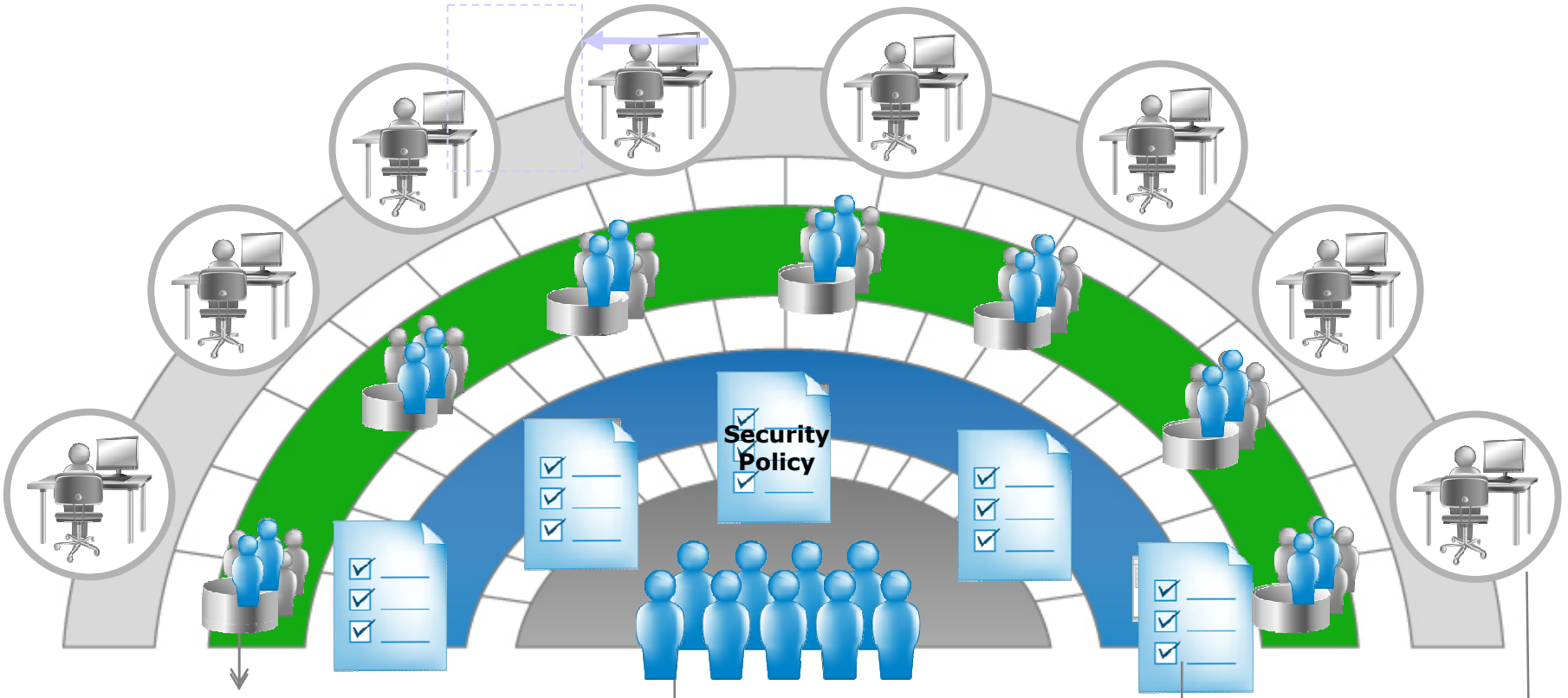


Alto custo de administração e suscetível a erros, fraudes, privilege creep

Risco pelo acúmulo de privilégios



Resolvendo...



IDENTIDADES
MUITAS IDENTIDADES
REDUZIDAS

- >Administração mais simples
- >Custos Reduzidos
- >Auditoria melhorada para facilitar compliance

MUITOS USUÁRIOS

- > Single Sign-on
- > Self-service

MUITAS APLICAÇÕES

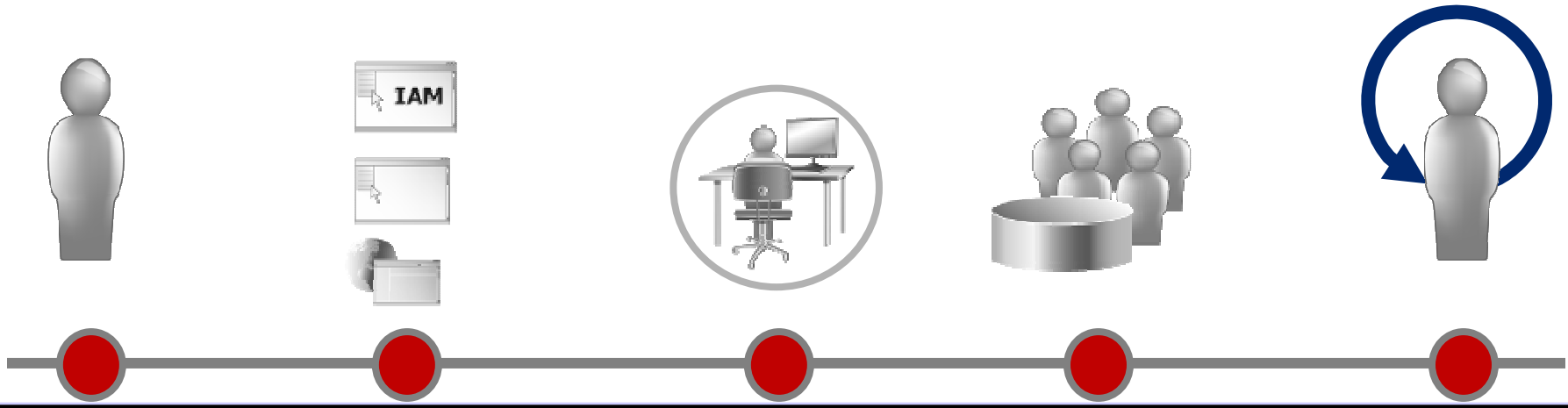
- >Segurança Centralizada
- >Desenvolvimento de apps mais fácil

ADMINISTRAÇÃO
CENTRAL
MUITAS ILHAS

- >Custos administrativos reduzidos
- >Administração consistente
- >Automação dos processos

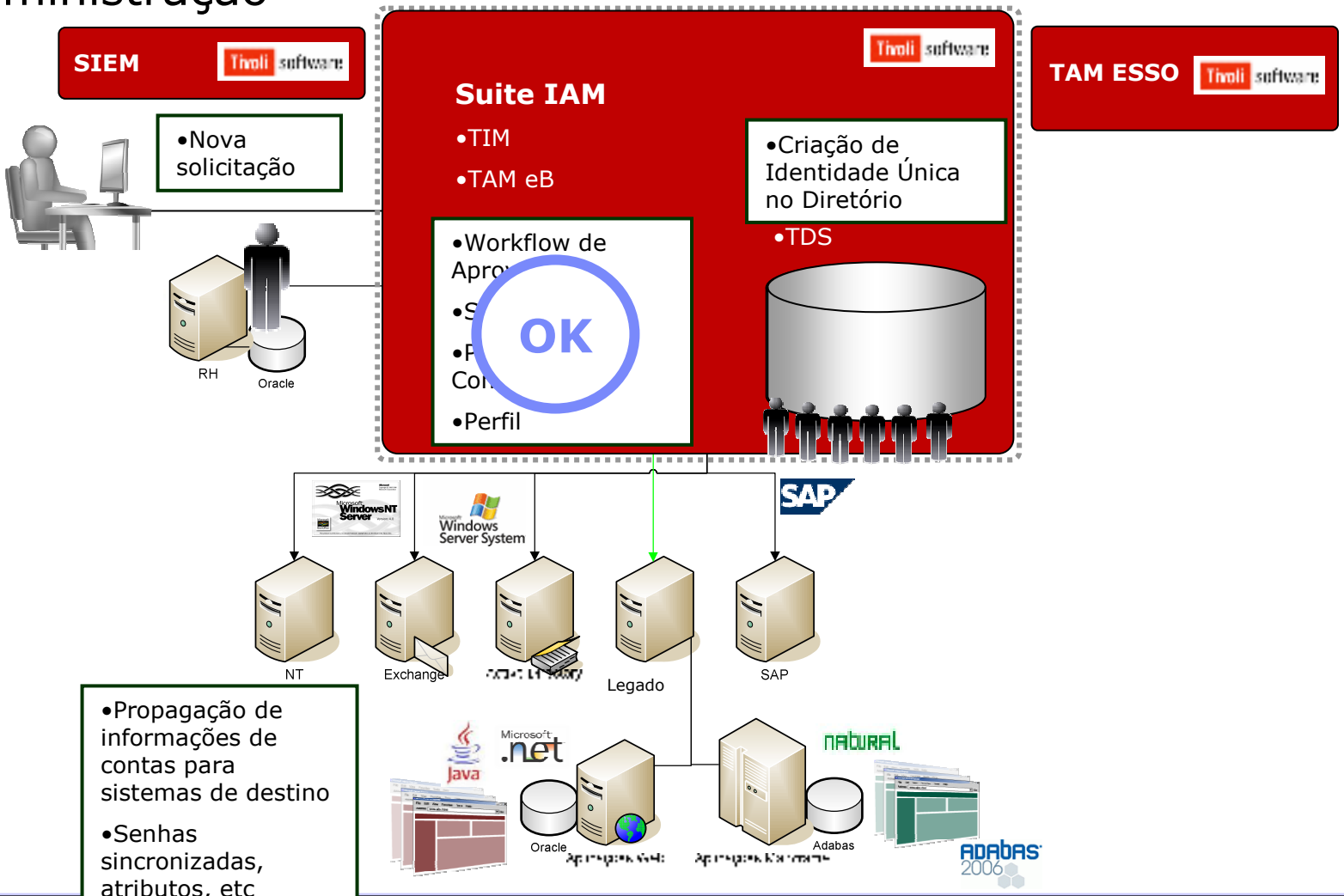
Processo de IAM unificado
A: Administração

- Gestão de Identidades, Provisionamento e Acesso
  - 1 – Automatizar a criação da Identidade Global (Integração com RH, fluxo de férias, suspensões, demissões)
  - 2 – Padronizar, unificar e automatizar o processo de acesso a aplicações (Access Control)
  - 3 – Delegar a administração de usuários e seus respectivos acessos (Habilitar portal de gestão)
  - 4 – Gerenciar acessos e privilégios (quem acessa qual aplicação, via portal de Gestão)
  - 5 – Habilitar Self-Service para o usuário final (via portal de Self-Service, Workflow)

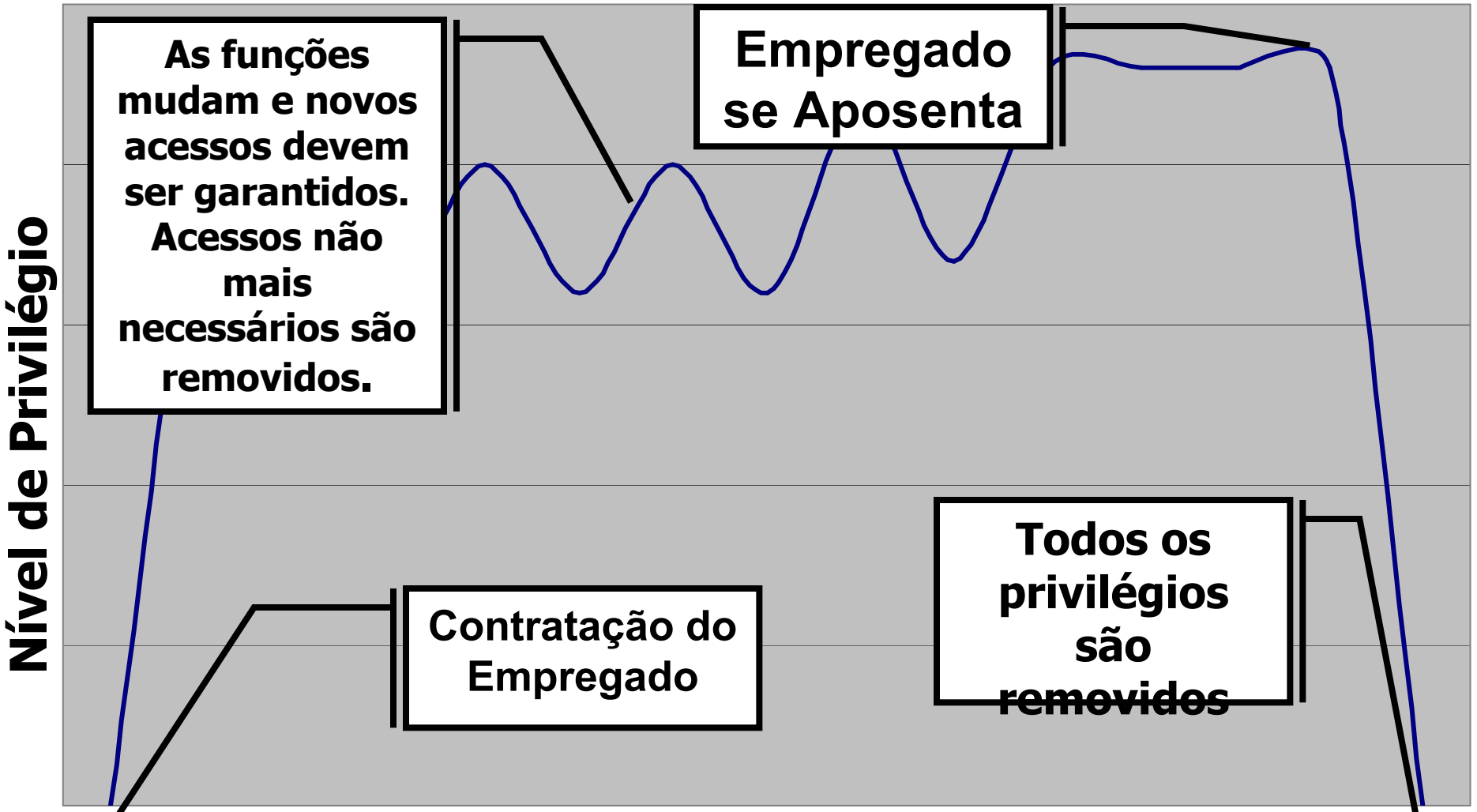


Processo de IAM unificado

A: Administração

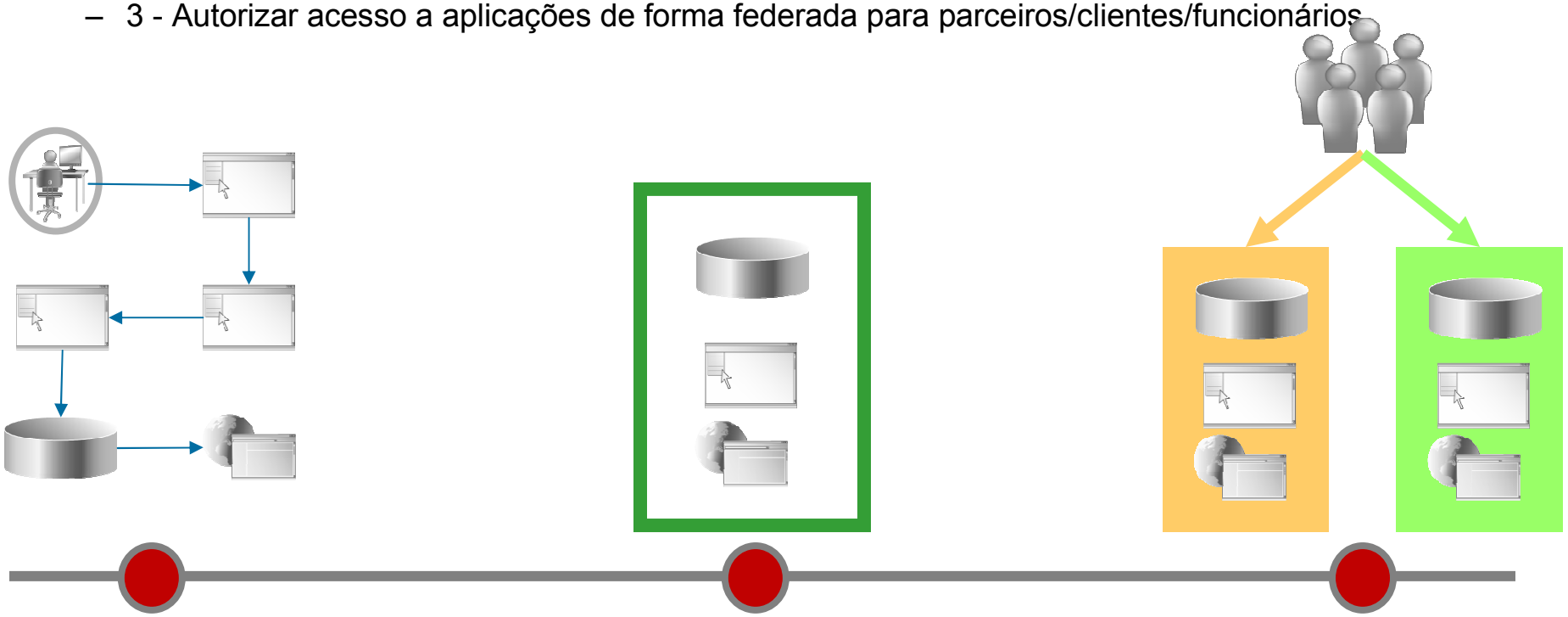


Ciclo de vida de usuários com IAM



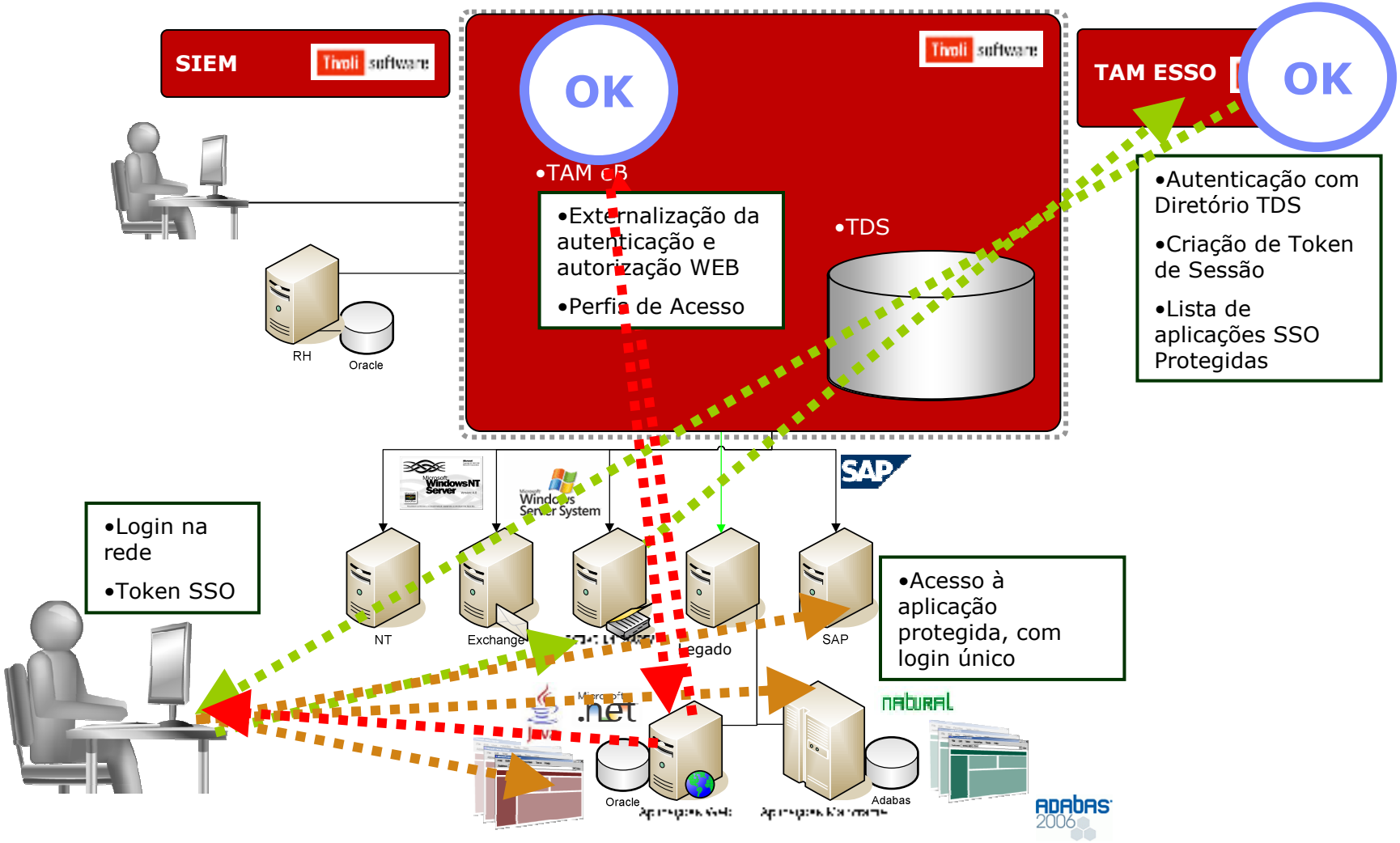
Processo de IAM unificado
A: Autenticação, A: Autorização

- Controle de Acessos e Autenticação
  - 1 - Definir fluxo seguro e automático para autenticação em aplicações (SSO)
  - 2 - Proteger acesso a recursos críticos do Sistema Operacional
  - 3 - Autorizar acesso a aplicações de forma federada para parceiros/clientes/funcionários



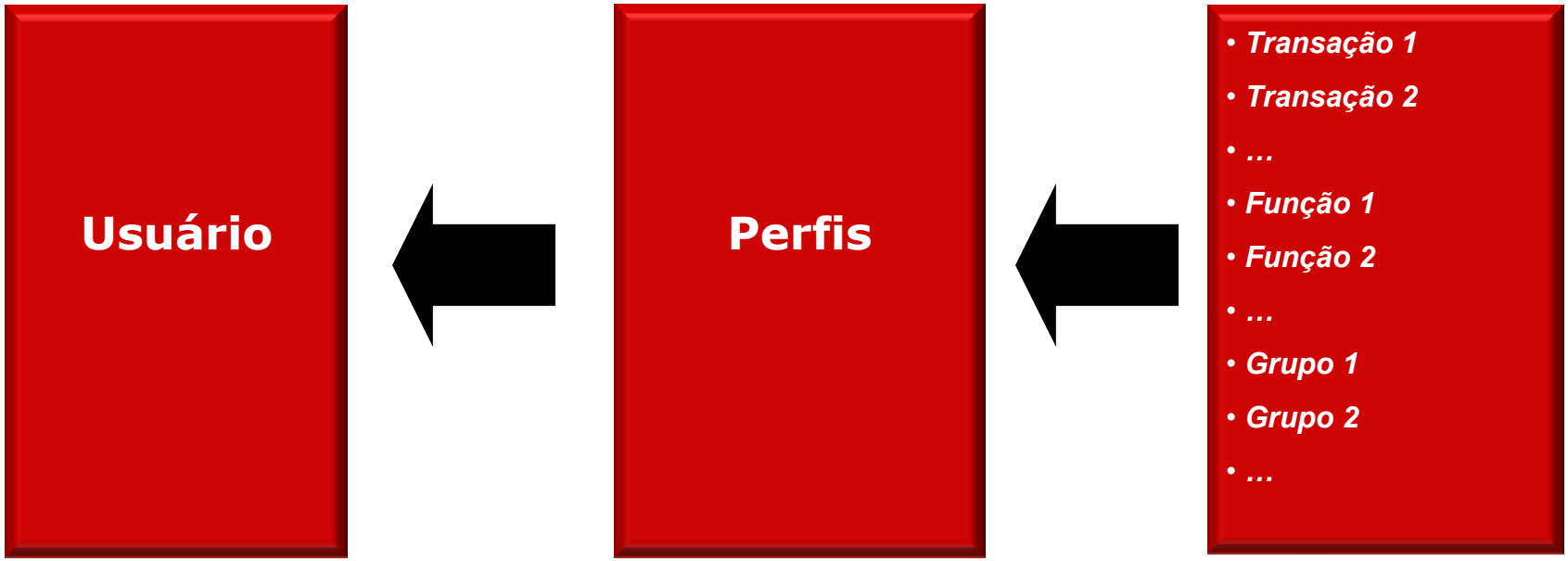
Processo de IAM unificado

A: Autenticação, A: Autorização



Modelo ideal de concessão de acesso

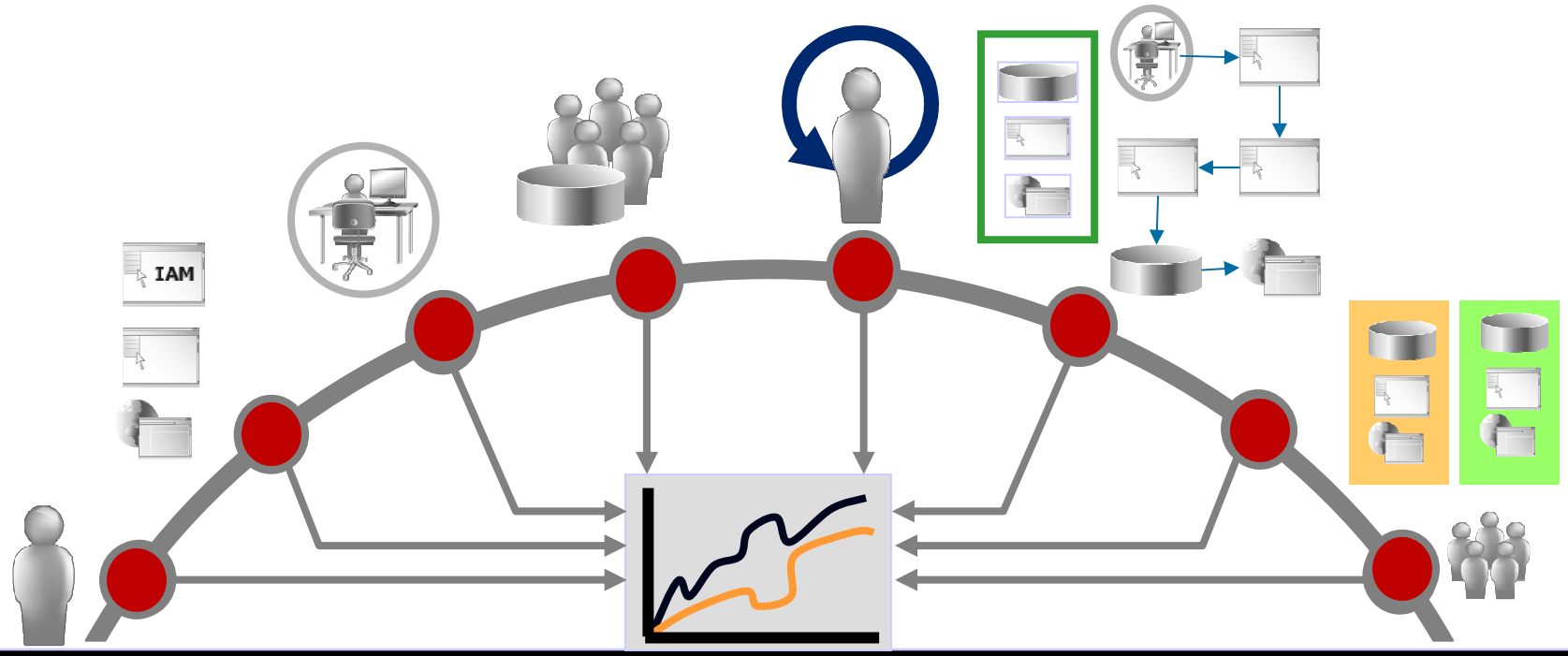
RBAC: Role Based Access Control



Menor custo e menor risco de erros

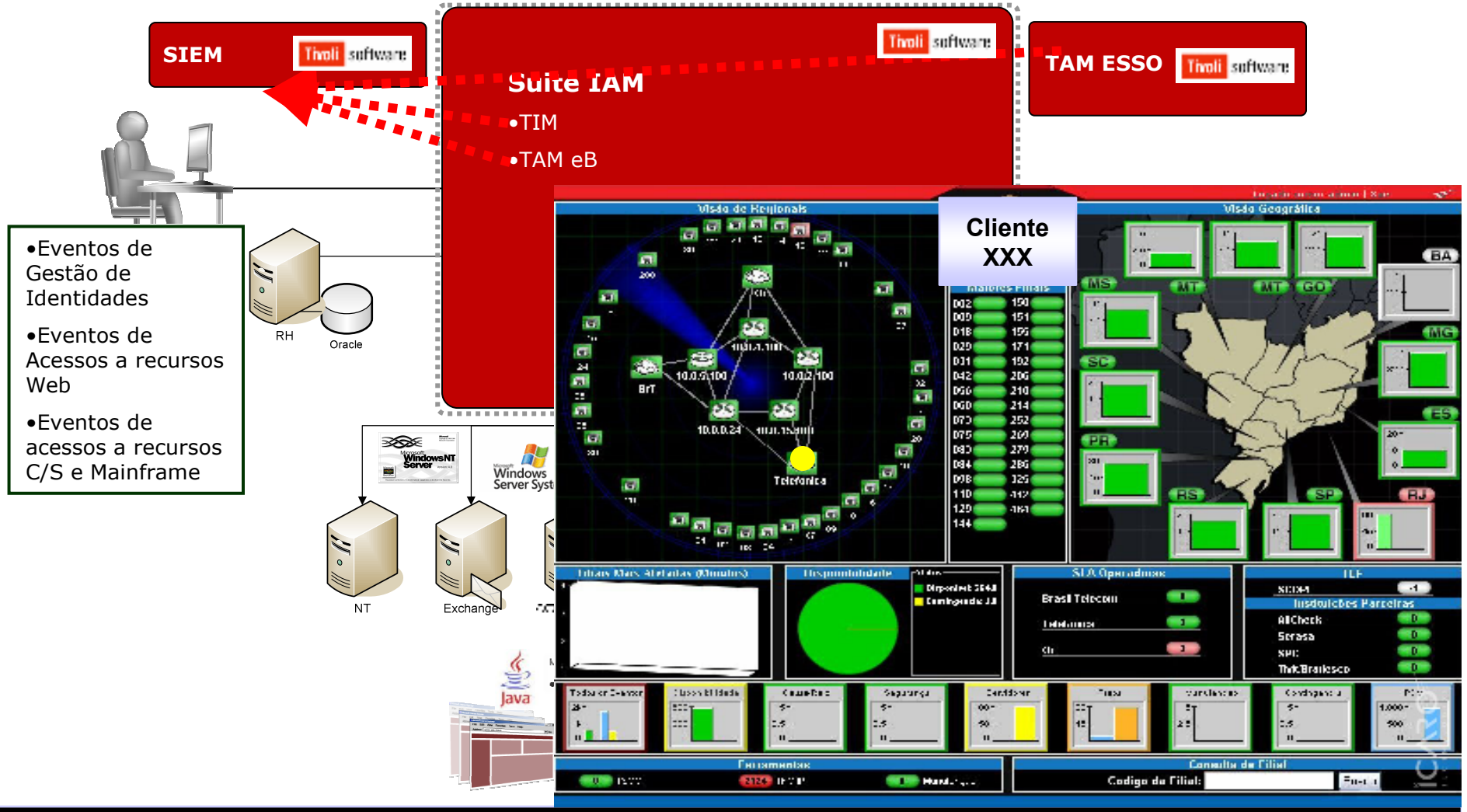
Processo de IAM unificado
A: Auditoria

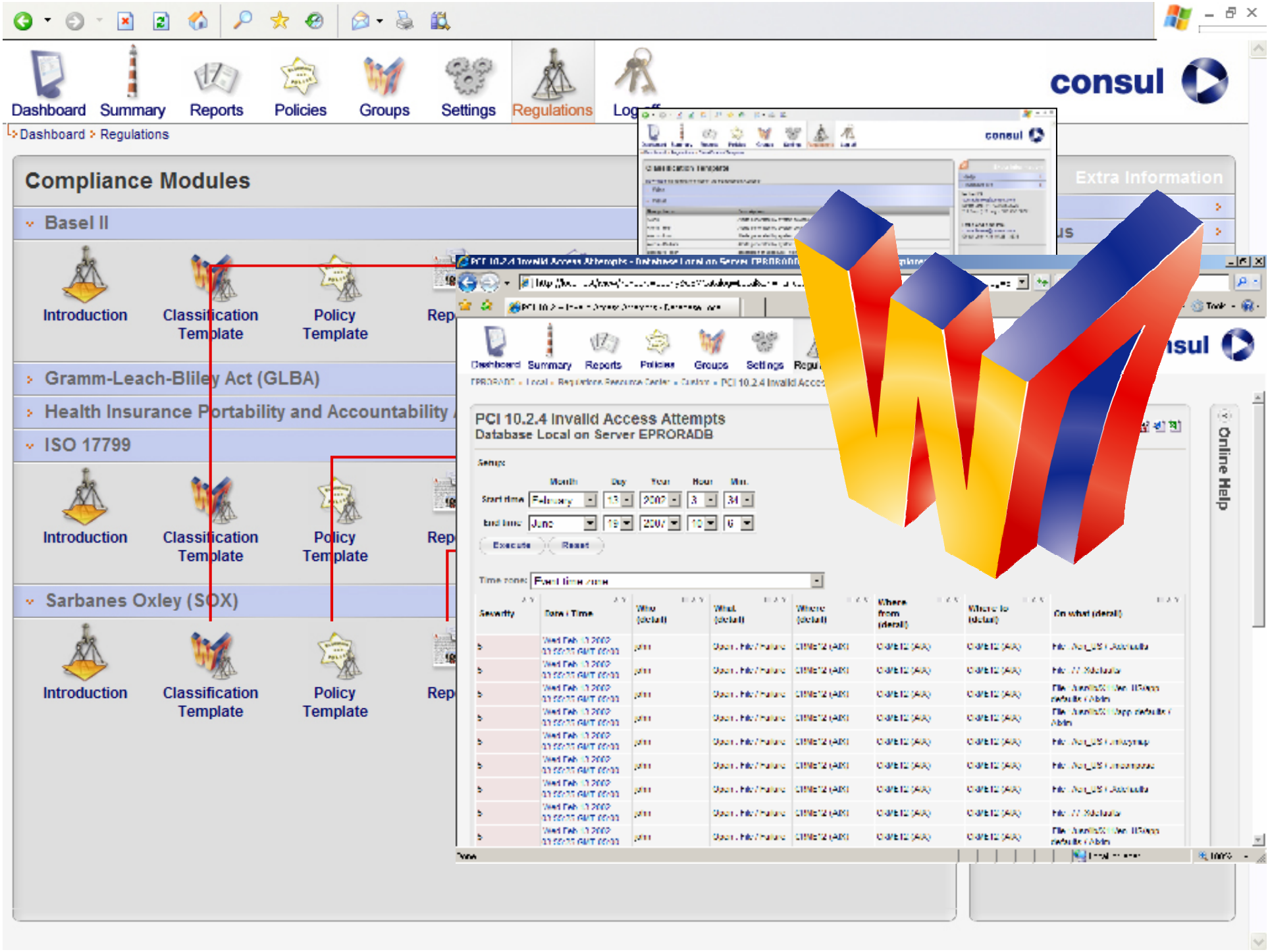
- Auditoria, Monitoração e Governança
  - Monitorar todos os eventos relacionados à identidade e aos acessos (operações)
  - Consolidar informações de compliance, disponibilizar relatórios e portais de conformidade contínua



Processo de IAM unificado

A: Auditoria




Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
consul
Dashboard › Regulations
Compliance Modules
Extra Information
Basel II
Introduction
Classification Template
Policy Template
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability
ISO 17799
Introduction
Classification Template
Policy Template
Sarbanes Oxley (SOX)
Introduction
Classification Template
Policy Template
PCI 10.2.4 Invalid Access Attempts
Database Local on Server EPRORADB
Online Help

Considerações importantes para IAM

Problemas comuns

- Proteger todas as plataformas (mainframe e distribuída)
- Solução incompleta e/ou não integrada
- Integração com sistemas externos de TI, e de negócio
- Usuário final não enxerga benefícios
- Escalabilidade
- Administradores, gestores não enxergam benefícios

Medidas

- Garantir consistência da segurança (padrões)
  - Evitar soluções pontuais e integrações complexas, definir escopo e fronteiras
  - Preservar investimentos passados, viabilizar através de XML, SOA, Webservices (reuso)
  - Viabilizar Self-service, Single sign-on para web e aplicações corporativas. Security Awareness
- Casos de referência de sucesso
  - Definir Quick-Wins factíveis em 6 meses (ex: Single Sign-On VIP, Self-Service), Security Awareness

Considerações importantes para IAM

Problemas comuns

- Mapear Perfis primeiro, ou instalar a ferramenta?
- Redesenhar processos ou implementar atuais, AS-IS
- Reescrever código de todas as aplicações legadas
- Desenvolver conectores para todas as aplicações legadas
- Problemas de disponibilidade, bugs, suporte, unha encravada
- Gestores AINDA não enxergam benefícios

Medidas

- Projetos integrados. Definir Roles de provisionamento básicas, para quick-win
- Realizar assessment de IAM antes
- Análise de custo beneficio: Integrar ao processo de IdM ou ao de Access Mgmt, ou não integrar a nada!
- Análise de custo beneficio: Integrar ao processo de IdM ou ao de Access Mgmt, ou não integrar a nada!
- Escolha de fornecedor, treinamento, serviços profissionais, definição de owner
- Escopo/necessidades/expectativas precisariam ser definidos mais claramente

Lições Aprendidas

- Acuracidade das nformações provenientes das fontes autoritativas do RH
- Aprender com os erros e agir rápido
- Importância dos Fluxos de Processos de TI
- Time é Tudo – Comunicação (interna e usuários)
- Estratégia de longo prazo, resultados no curto prazo

IBM Security Forum

Soluções para um ambiente seguro

Os 4 A's do IAM e o Pre-Crime

Obrigado!

Henrique Bernardes, CISM, CISSP
Tivoli Security Sales Manager
Bernardes@br.ibm.com