



Universidade de São Paulo
B R A S I L



Universidade de São Paulo
Centro de Computação Eletrônica

*“Ferramenta SiRI e sua utilização pela Equipe de
Segurança da USP”*

Apresentação:

Mauro Cesar Bernardes

Rafael Nogueira Tavares

Abril de 2003

Estrutura da Apresentação

➤ **Motivação**

⇒ Uma visão geral da USPNet

⇒ A Equipe de Segurança

⇒ O cenário antigo

➤ **A ferramenta SiRI**

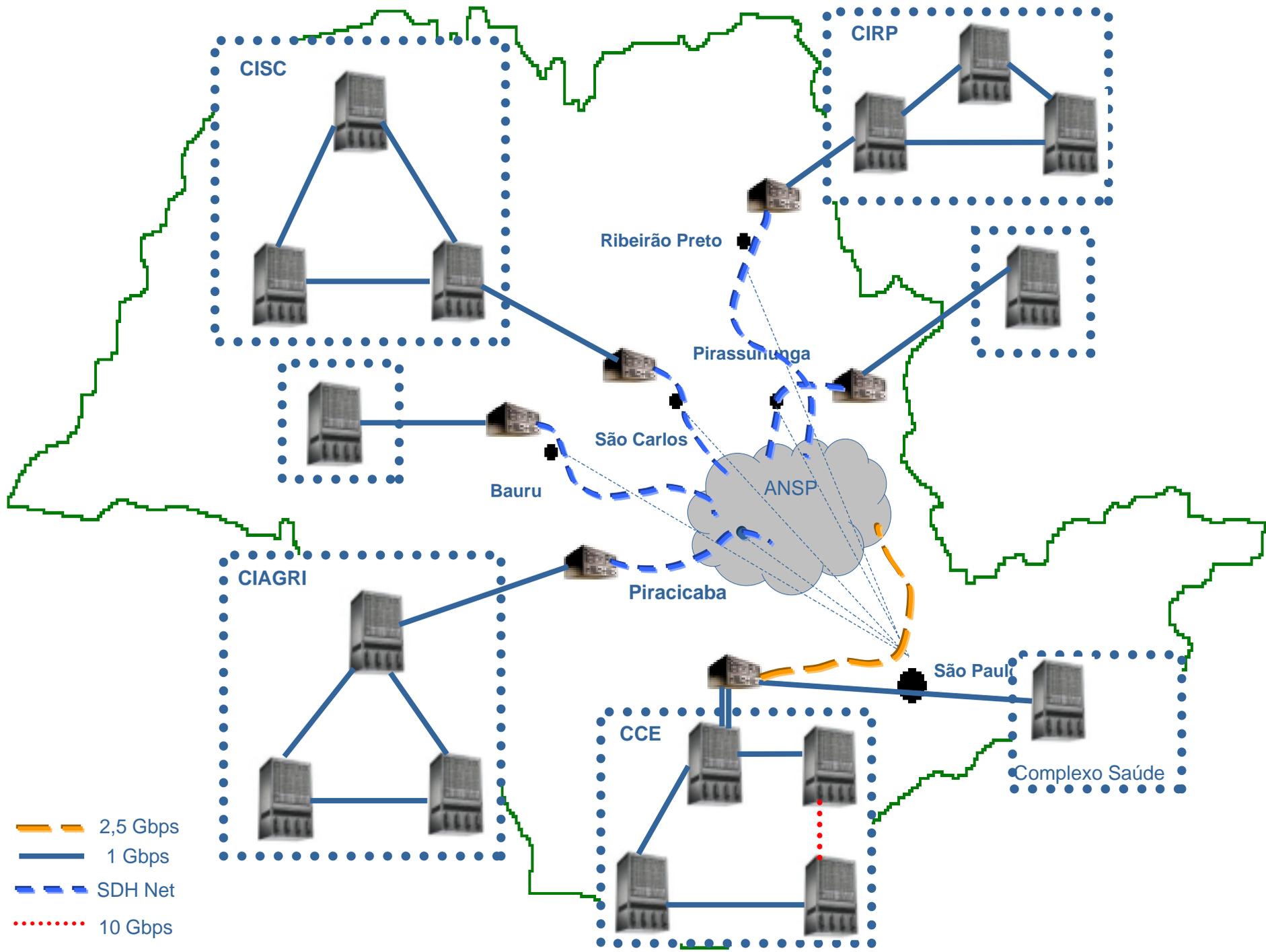
⇒ Funcionalidades da Ferramenta

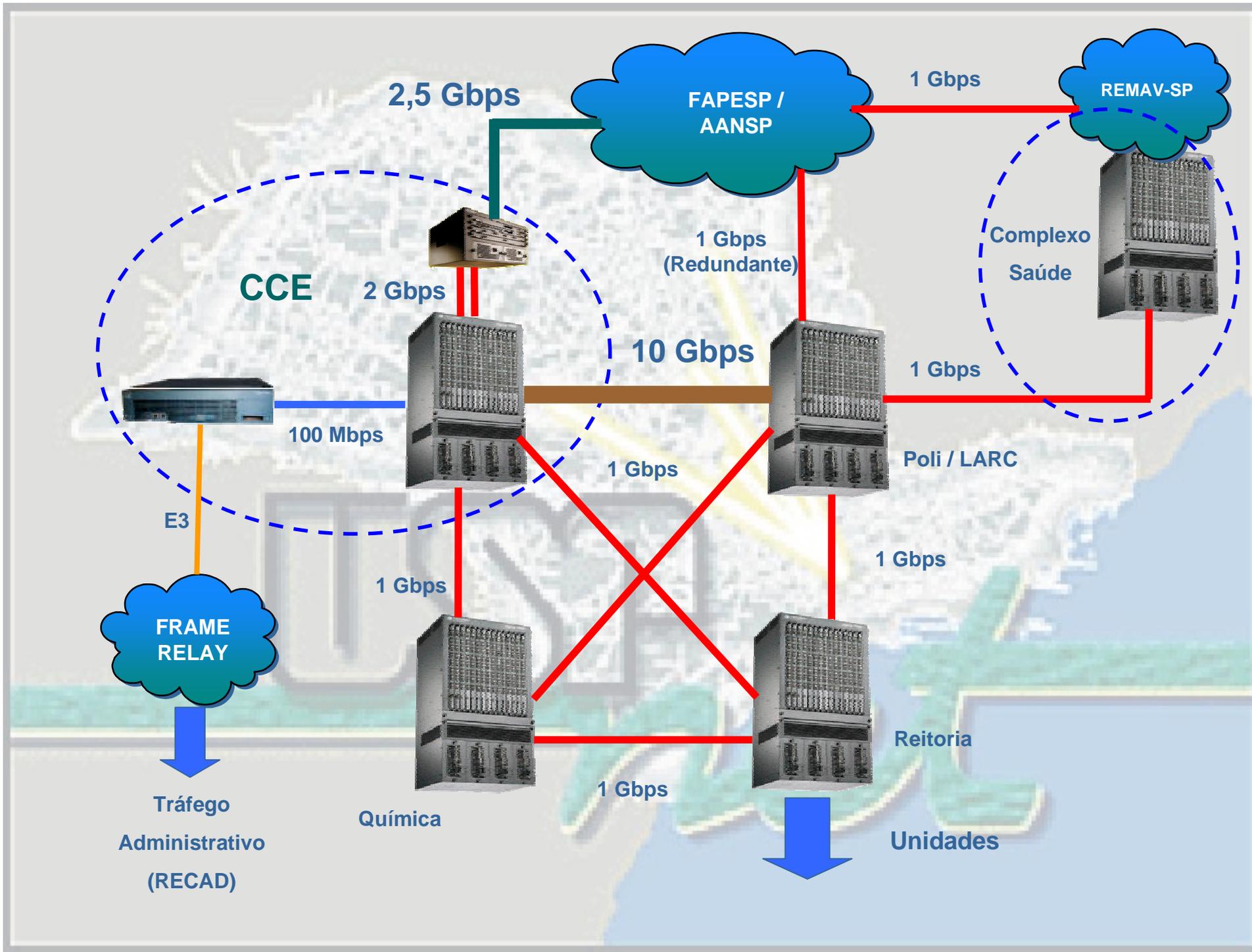
⇒ O cenário atual

➤ **Trabalhos futuros**

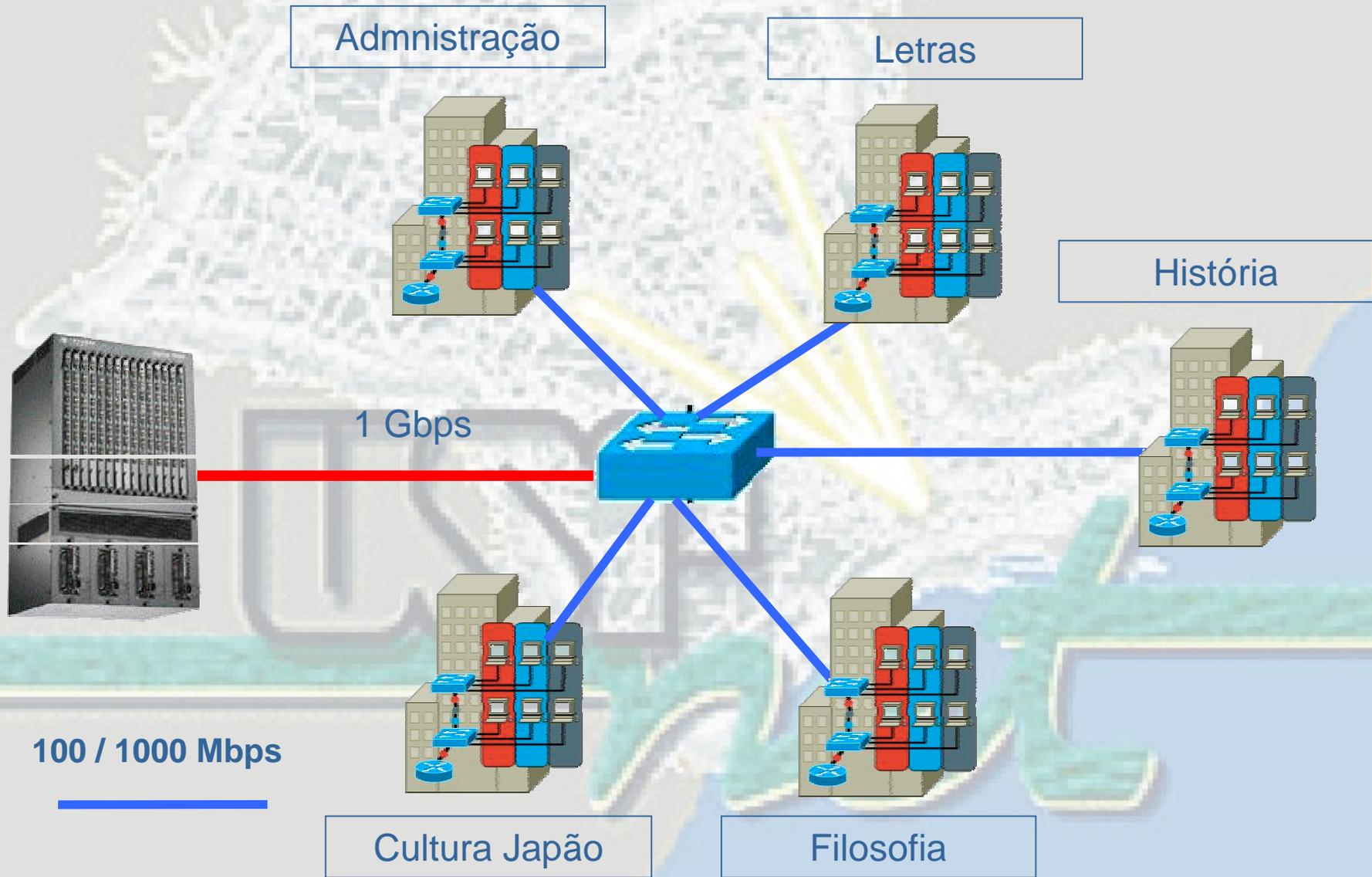
➤ **Debate.**

Uma visão Geral da USPNet





Visão Geral do Campus São Paulo



A Equipe de Segurança

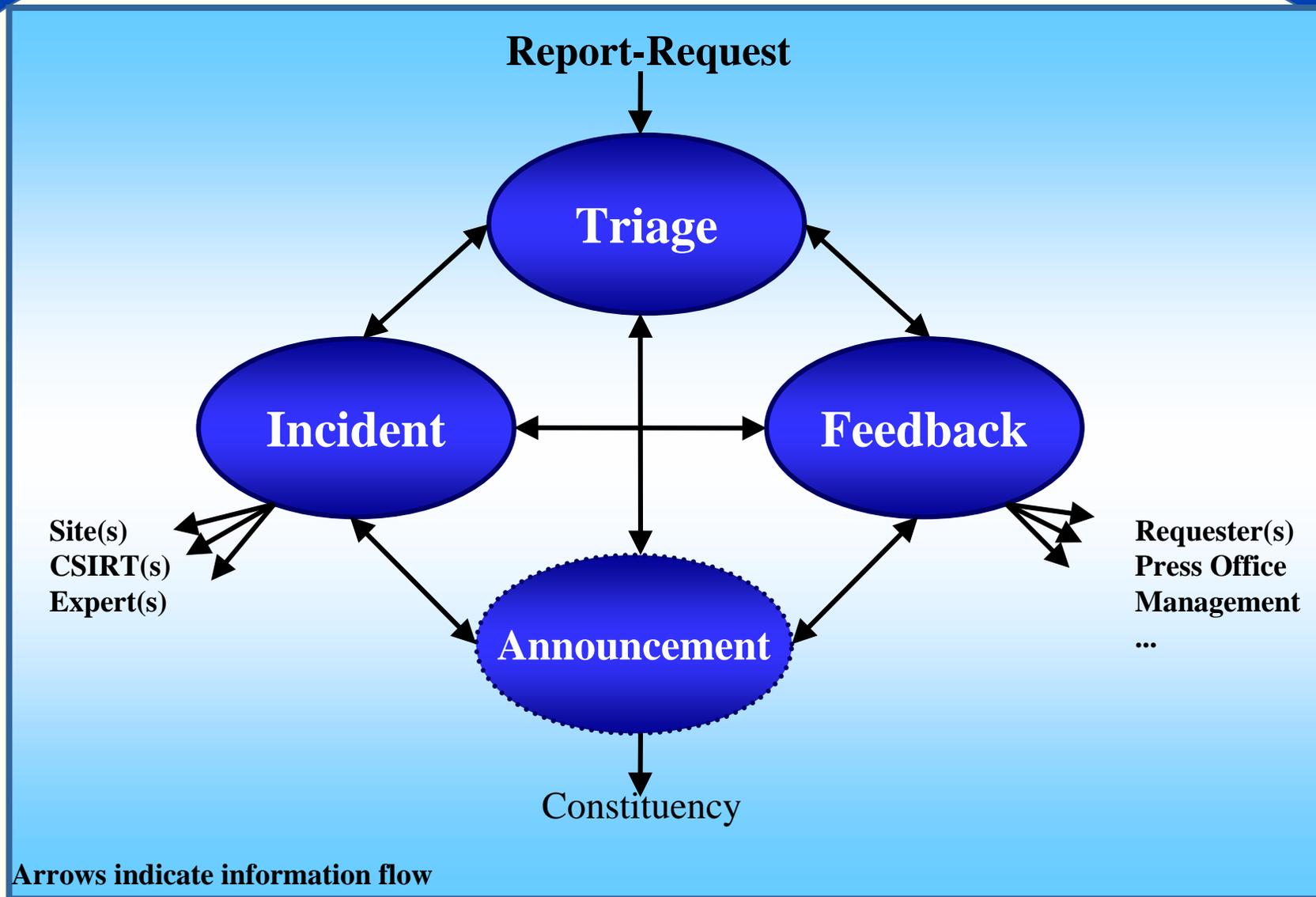
➤ Centro de Computação Eletrônica

- ⇒ Responsável pelo security@usp.br, abuse@usp.br, ...
- ⇒ 4 Analistas
- ⇒ 4 Técnicos/operadores
- ⇒ Atendimento 24x7

➤ Administradores em cada Unidade

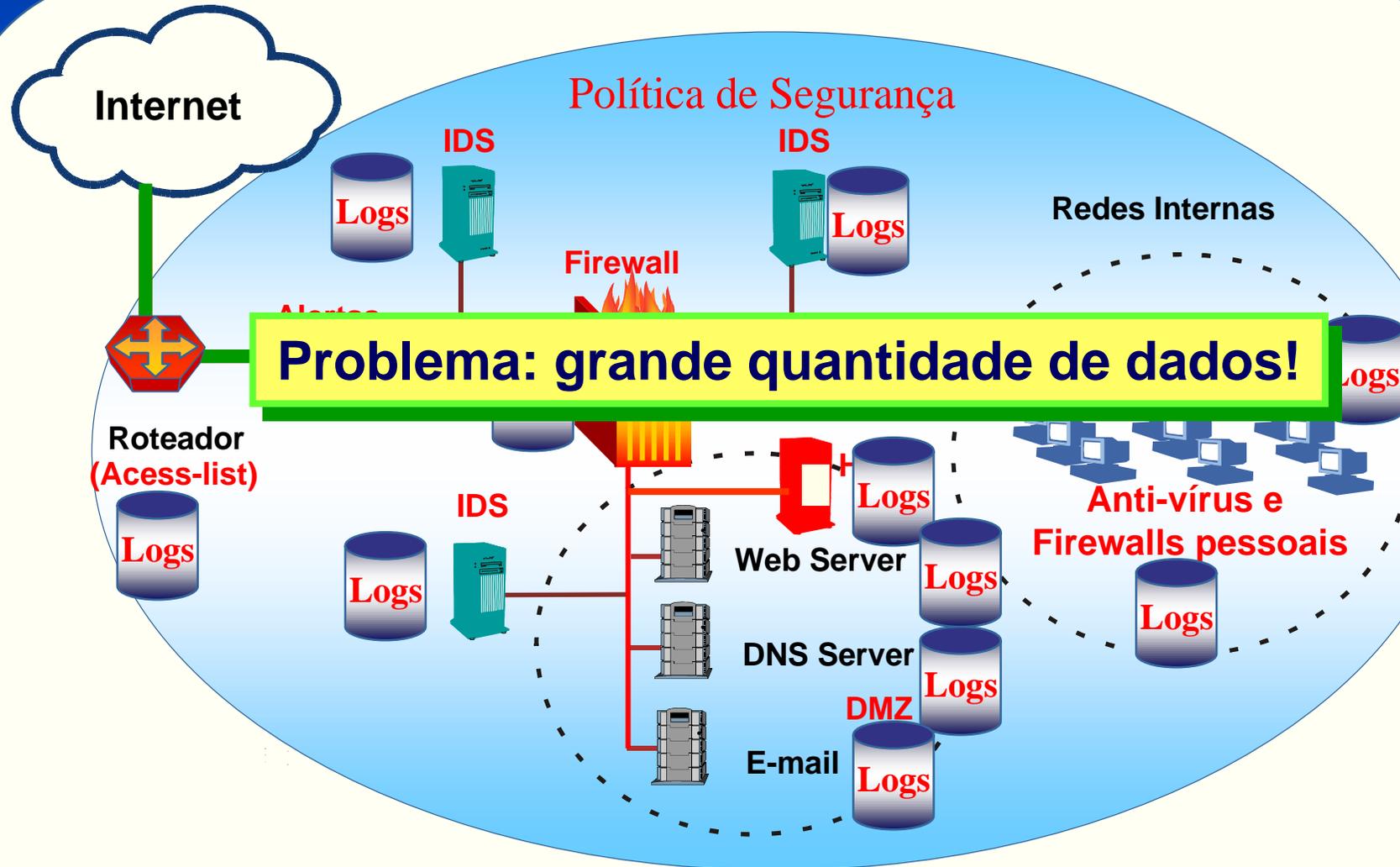
➤ Trabalho cooperativo e colaborativo

IR Service Functions Overview



Fonte: <http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>

Problemas no cenário antigo



“O problema onde há um excesso de dados pode ser tão prejudicial quanto a sua falta”

A Ferramenta SiRI

A Ferramenta SiRI

São Paulo,
06 de Abril de 2003

Acesso ao SiRI

Login:
Senha:

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança

E-mail:
 Cadastrar
 Descadastrar

Últimos Alertas

- Remote Buffer Overflow in Sendmail WORM_LOVGATE.C
- MS-SQL Server Worm

USP Universidade de São Paulo BRASIL

CSIRT - Computer Security Incident Response Team

Sobre o SiRI Conheça mais sobre o projeto SiRI.	Boletim de Alertas Boletim destinados aos administradores de sistemas da USP, cadastre-se já.	Alertas Últimos alertas segurança.
Procedimentos Procedimentos para o dia-a-dia dos administradores de sistemas.	Gráficos Gráficos dos reports recebidos pela USP nos últimos meses.	Manual de Operação Manual de operação do sistema.

Minimização do Tempo de RI

Home Sobre o SIRI Procedimentos Alertas Gráficos Manual de Operação

São Paulo,
06 de Abril de 2003

Logon: Mauro Cesar Bernardes

Sistema de Resposta a Incidentes

Incidentes em Aberto

Análise:	0	
Administrador:	0	
Reclamante:	0	
Abertos na data de Hoje:	0	
Encerrados na data de Hoje:	0	
Expirados:	3	

| Incidentes | Alertas | Servidores | Gráficos |

Atenção, existem Incidentes expirados !!!

Os Incidentes abaixo estão excederam a data limite de resolução !!!

Incidente	Tipo	Status	Data/Hora	Status	Log	Mail
1-032003	Mau Uso	Expirado	2003-02-27/21:03:50			
2-032003	Spam	Expirado	2003-02-27/21:03:00			
6-032003	Spam	Expirado	2003-03-06/13:25:53			

Fechar

Triagem de um Incidente

São Paulo,
06 de Abril de 2003

Acesso ao SIRE
Login: m0ss0r
Senha:

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança
E-mail:
 Cadastrar
 Descadastrar

Últimos Alertas
Remote Buffer
Overflow in Sendmail
WORM_LOVGATE.C
MS-SQL Server Worm

Cadastro de Incidente

Dados do Incidente	
Tipo do Incidente:	Spam
IP (USP) Envolvido:	143.107.xxx.xxx
Unidade Envolvida:	CCE
Para enviar e-mail notificando o Administrador, clique aqui <input type="checkbox"/>	
Dados do Reclamante	
Nome do Reclamante:	XYZ
E-mail do Reclamante:	xyz@dominio.com
IP do Reclamante:	xxxxxxx.xxx
Para notificar o Reclamante, clique aqui <input type="checkbox"/>	
Lingua: <input type="radio"/> Português <input checked="" type="radio"/> Inglês	
Informações do Incidente:	
<input type="text" value="Acrescentar informações complementares e fornecidas pelo reclamante e que poderão ser úteis à equipe de segurança e aos administradores responsáveis pelas máquinas envolvidas"/>	
Data do Incidente	
Data do Incidente:	2003/04/06
Hora do Incidente:	11:57:32
Dados do Técnico	
Incidente Registrado por:	Meuro Cesar Bernardi
<input type="button" value="Cadastrar"/>	

| [Menu](#) | [Opções](#) |

Ações Emergenciais

- **A partir da triagem do Incidente, pode-se adotar ações emergenciais.**

Notificações Personalizadas

Envio de Mail - Microsoft Internet Explorer

Envio de Notificação

Dados do E-mail	
Número do Incidente:	1-032003
Nome do Administrador:	Cristian
E-mail do Administrador:	christian@telefutura.com
Cc:	security@usp.br
Mensagem:	<p>Prezado(s) Administrador(es),</p> <p>Teríamos algum posicionamento referente ao incidente 1-032003?</p> <p>Para visualizar o incidente clique no link abaixo:</p> <p>http://gandalf.uspnet.usp.br/~rafael/incidentes/visualiza_incidente.php?incid_cod=1-032003</p> <p>Atenciosamente,</p>
<input type="button" value="Enviar"/> <input type="button" value="Fechar Janela"/>	

Identificação única para cada Incidente

Home Sobre o SIRI Procedimentos Alertas Gráficos Manual de Operação

São Paulo,
06 de Abril de 2003

Acesso ao SIRI
Login: m0ss0r
Senha:

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança
E-mail:
 Cadastrar
 Descadastrar

Últimos Alertas
Remote Buffer
Overflow in Sendmail
WORM_LOVGATE.C
MS-SQL Server Worm

Cadastro de Incidente
Incidente Cadastrado com sucesso !!!

Dados do Incidente	
Número do Incidente:	7-042003
Tipo do Incidente:	Spam
IP USP Envolvido:	143.107.xxx.xxx
Data de expiração:	2003-04-09
Data de encerramento:	2003-04-21
IP do Reclamante:	X Y Z
Data do Incidente:	2003/04/06
Hora do Incidente:	11:57:32
Data do Cadastro do Incidente:	2003-04-06
Hora do Cadastro do Incidente:	11:57:32
Incidente Registrado por:	Mauro Cesar Bernardes

[| Menu Opções |](#)

Visão Geral das Opções para Incidentes

São Paulo,
06 de Abril de 2003

Acesso ao SIRS

Login: mcesar
Senha:

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança

E-mail:

Cadastrar
 Descadastrar

Últimos Alertas

- Remote Buffer Overflow in Sendmail
- WORM_LOVGATE.C
- MS-SQL Server Worm

Gerenciamento de Incidentes de Segurança

Cadastro de Incidentes	
Cadastro	
Consulta de Incidentes	
Por Data	Por Mês
Por Tipo	Por Status
Números	
Em Aberto / Encerrados	-
Alteração de Incidentes	
Alteração	Alteração de Status
Log de Incidentes	
Inclusão	Consulta

[Página Principal](#)

Acompanhamento do Incidente

São Paulo,
05 de Abril de 2003

Acesso ao SIRE

Login: mcesar
Senha:

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança

E-mail:
 Cadastrar
 Descadastrar

Últimos Alertas

- Remote Buffer Overflow in Sendmail
- WORM_LOVGATE.C
- MS-SQL Server Worm

Home Sobre o SIRE Procedimentos Alertas Gráficos Manual de Operação

Busca de Incidentes por Data

Digite a Data no formato (aaaa-mm-dd):

Foram encontrada(s) 1 ocorrência(s) !!!

Incidente	Data	Hora	Tipo	Status	Criador	Log
7-042003	2003-04-06	11:57:32	Spam	Administrador	Mauro Cesar Bernardes	

| [Menu Opções](#) |

Acesso Mediante Certificação

Acompanhamento do Incidente

Microsoft Internet Explorer

Acompanhamento de Incidente

Número do Incidente: Consultar

Dados do Incidente:

Número: 7-042003	Tipo: Spam	Status: Administrador
Data: 2003-04-06	Data Cadastro: 2003-04-06	
Hora: 11:57:32	Hora Cadastro: 11:57:32	
Reclamante: X Y Z	E-mail do Reclamante: xyz@dominio.com	
IP USP: 143.107.xxx.xxx	IP Reclamante: xxx.xxx.xxx.xxx	
Expira: 2003-04-09	Encerra: 2003-04-21	
Criador: Mauro Cesar Bernardes		
Logs:		
<p>Acrescentar informações complementares e fornecidas pelo reclamante e que poderão ser úteis à equipe de segurança e aos administradores responsáveis pelas máquinas envolvidas</p>		

Não existem Logs para este incidente !!!

[Consulta outro incidente](#) | [Menu Opções](#)

Informações de Acompanhamento

Home Sobre o SIRI Procedimentos Alertas Gráficos Manual de Operação

São Paulo,
05 de Abril de 2003

Acesso ao SIRI
Login: mosseser
Senha:
Login
Quero me cadastrar!
Esqueci minha senha!

Boletim de Segurança
E-mail:
 Cadastrar
 Descadastrar
Enviar

Últimos Alertas
Remote Buffer
Overflow in Sendmail
WORM_LOVGATE.C
MS-SQL Server Worm

Inclusão de Log de Incidente

Dados do Incidente:
Incidente: 7-042003 Validar

Informações do Log
Informação: Logs e informações complementares!
Cadastrar

| Menu Opções |

Informações de Acompanhamento

São Paulo,
06 de Abril de 2003

Acesso ao SIRS
Login: mcasar
Senha: xxx

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança
E-mail:
 Cadastrar
 Decadastrar

Últimos Alertas
Remote Buffer Overflow in Sendmail
WORM_LOVGATE.C
MS-SQL Server Worm

Acompanhamento de Incidente

Número do Incidente:

Dados do Incidente:

Número: 7-042003	Tipo: Spam	Status: Administrador
Data: 2003-04-06	Data Cadastro: 2003-04-06	
Hora: 11:57:32	Hora Cadastro: 11:57:32	
Reclamante: X Y Z	E-mail do Reclamante: xyz@dominio.com	
IP USP: 143.107.xxx.xxx	IP Reclamante: xxx.xxx.xxx.xxx	
Expira: 2003-04-09	Encerra: 2003-04-21	
Criador: Mauro Cesar Bernardes		
Logs:		
<input type="text" value="A acrescentar informações complementares e fornecidas pelo reclamante e que poderão ser úteis à equipe de segurança e aos administradores responsáveis pelas máquinas envolvidas"/>		

Dados de Log do Incidente

Log Número:	1
Criador:	
Data do Log:	06/04/2003
Hora do Log:	12:09:22
Descrição do Log:	Logs e informações complementares!

[Consulta outro incidente](#) | [Menu Opções](#)

Consultas personalizadas para a Equipe

The screenshot shows a web application interface with a navigation menu at the top: Home, Sobre o SIBI, Procedimentos, Alertas, Gráficos, and Manual de Operação. The main content area is titled "Consulta Incidente".

On the left side, there is a sidebar with the following sections:

- São Paulo, 06 de Abril de 2003**
- Acesso ao SIBI**: Login field with "mcesar", Password field with "***", and a "Login" button. Links for "Quero me cadastrar!" and "Esqueci minha senha!" are also present.
- Boletim de Segurança**: Email field, "Cadastrar" and "Descadastrar" radio buttons, and an "Enviar" button.
- Últimos Alertas**: A list of alerts including "Remote Buffer Overflow in Sendmail", "WORM_LOVGATE-1", and "MS-SQL Server Worm".

The main content area contains a form to select the incident type, with "Spam" selected in a dropdown menu. A "Submeter" button and an "Encerrados" checkbox are also visible.

Below the form, the text "Foi(ram) encontrada(s) 3 ocorrência(s) !" is displayed. A table shows the results of the query:

Número	Data	Condição	IP	Status	Log
2-032003	2003-02-27	POLI	-	Expirado	
6-032003	2003-03-06	IQ	143.106.10.xxx	Expirado	
7-042003	2003-04-06	CCE	xxx.xxx.xxx.xxx	Expirado	

At the bottom of the main content area, there is a link for "Menu Opções".

Refinamento das informações do Incidente

Alteração de Incidente

Incidente Número:

Dados do Incidente

Incidente Número:

Dados do Reclamante

Nome Recl.:

E-mail Recl.:

Data e Horas do Incidente

Data Incidente:

Hora Incidente:

Informações:

A acrescentar informações complementares e fornecidas pelo reclamante e que poderão ser úteis à equipe de segurança e aos administradores responsáveis pelas máquinas envolvidas

IP USP do Incidente:

IP Reclamante:

Data Cad. Incidente:

Hora Cad. Incidente:

Status do Incidente:

Criador do Status:

Alteração de Status

The screenshot shows a web browser window displaying a web application. The browser's address bar is empty, and the page title is "Alteração de Status de Incidente". The page has a navigation menu at the top with links: "Home", "Sobre o SIRE", "Procedimentos", "Alertas", "Gráficos", and "Manual de Operação".

On the left side, there is a sidebar with the following sections:

- São Paulo, 06 de Abril de 2003**
- Acesso ao SIRE**
 - Login: mcesar
 - Senha: ***
 - Login
 - Quero me cadastrar!
 - Esqueci minha senha!
- Boletim de Segurança**
 - E-mail: [input field]
 - Cadastrar
 - Descadastrar
 - Enviar
- Últimos Alertas**
 - Remove Buffer Overflow in Sendmail
 - WORM_LOVGATE.C
 - MS-SQL Server Worm

The main content area is titled "Alteração de Status de Incidente" and contains a form with the following fields:

- Número do Incidente: [input field] Submeter
- Status incidente:**
- Incidente: 7-042003
- Data do incidente: 06/04/2003
- Hora do incidente: 11:57:32
- Tipo de Incidente: Spam
- Data de Expiração: 2003-04-09
- Data de Encerramento: 2003-04-21
- Status do Incidente:** Administrador
- IP Reclamante: XXX.XXX.XXX.XXX
- IP USP Envolvido: 143.107.XXX.XXX
- Criado por: Mauro Cesar Bernardes
- Status para ser alterado: Análise (dropdown menu)
- Notas: [text area]
- Alterar

At the bottom of the form, there is a link: | [Menu Opções](#) |

Gerenciamento de Alertas

The screenshot shows a web browser window displaying the SIREM alert management interface. The browser's address bar shows the URL <http://www.sirem.gov.br>. The page has a navigation menu with links for Home, Sobre o SIREM, Procedimentos, Alertas, Gráficos, and Manual de Operação. The main content area is titled "Gerenciamento de Alertas de Segurança" and contains a menu with the following items:

- Cadastro de Alertas
 - Cadastro
- Consulta de Alertas
 - Por Data
 - Por Mês
- Procedimentos
 - Cadastro
 - Consulta

Below the menu, there is a link for "Página Principal".

On the left side of the page, there is a sidebar with the following sections:

- São Paulo, 08 de Abril de 2003**
- Acesso ao SIREM**
 - Login:
 - Senha:
 -
 - [Quero me cadastrar!](#)
 - [Esqueci minha senha!](#)
- Boletim de Segurança**
 - E-mail:
 - Cadastrar
 - Decadastrar
 -
- Últimos Alertas**
 - Remote Buffer Overflow in Sendmail
 - WORM_LOVGATE.C
 - MS-SQL Server Worm

Cadastro de Alertas

São Paulo,
06 de Abril de 2003

Acesso ao SIRE

Login: mcesar
Senha: ***
Login

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança

E-mail:

Cadastrar
 Descadastrar

Enviar

Últimos Alertas

- Remote Buffer Overflow in Sendmail
- WORM_LOVGATE.C
- MS-SQL Server Worm

Cadastro de Alerta de Segurança

Dados do Alerta	
Nome:	XYZ WORM
Tipo:	Worm
Descrição:	Informações preliminares que descrevem o alerta
Nível:	Crítico
Link:	http://www.xyzalerta.com
Cadastrar	

| Página Principal |

Encaminhamento de Alertas

- **Alertas Classificados;**
 - ⇒ **Uso de Ontologias**
- **Alertas priorizados conforme necessidade dos usuários;**
 - ⇒ **Listas de Discussão X SiRI: O diferencial;**
 - ⇒ **Correlacionar alertas às necessidades;**
 - ⇒ **Meta: Trabalhar informações prévias, Histórico e Extração de conhecimento;**

Cadastro de Procedimentos

São Paulo,
06 de Abril de 2003

Home Sobre o SIRE **Procedimentos** Alertas Gráficos Manual de Operação

Procedimentos de Segurança

Cadastro de Procedimento	
Nome:	Procedimento XYZ
Descrição:	Alguns atividades a ser realizada pelos envolvidos
Arquivo:	E:\nauro\artigos\index <input data-bbox="1422 544 1534 571" type="button" value="Procurar..."/>
Enviar Boletim ?	<input checked="" type="radio"/> Sim <input type="radio"/> Não
<input data-bbox="1198 619 1279 646" type="button" value="Submit"/>	

[Página Principal](#)

Acesso ao SIRE
Login: mcesar
Senha: ***

[Quero me cadastrar!](#)
[Esqueci minha senha!](#)

Boletim de Segurança
E-mail:
 Cadastrar
 Descadastrar

Últimos Alertas
Remove Buffer Overflow in Sendmail
WORM_LOVGATE.C
NS-SQL Server Worm

Correlação Alertas X Procedimentos

The screenshot shows a web application interface with a navigation menu at the top: Home, Sobre o SiRI, Procedimentos, Alertas, Gráficos, and Manual de Operação. The main content area is titled "Procedimentos de Segurança" and features a section for "Últimos Procedimentos".

On the left sidebar, there is a login section for "Acesso ao SiRI" with fields for "Login" (mcesor) and "Senha" (***), a "Login" button, and links for "Quero me cadastrar!" and "Esqueci minha senha!". Below this is a "Boletim de Segurança" section with an "Email" field, "Cadastrar" and "Descadastrar" radio buttons, and an "Enviar" button. At the bottom of the sidebar is an "Últimos Alertas" section listing "Remote Buffer Overflow in Sendmail", "WORM_LOVGATE.C", and "MS-SQL Server Worm".

The "Últimos Procedimentos" section contains two entries:

Últimos Procedimentos		
Procedimento: Procedimento XYZ	Data: 2003-04-06 NOVO	Hora: 12:04:03
Descrição: Alguma atividade a ser realizada pelos envolvidos		
Enviado por: Mauro Cesar Bernardes		
Download: index.htm		
Procedimento: Manual de Segurança do Windows 2000	Data: 2003-02-28	Hora: 09:02:30
Descrição: Manual indicado pela Microsoft para configuração do Windows 2000 com segurança.		
Enviado por: Rafael Tavares		
Download: SOG_download.pdf		

At the bottom of the main content area, there is a link: | [Página Principal](#) |

Correlação Alertas X Procedimentos

The screenshot displays a web application interface with a navigation menu at the top: Home, Sobre o SIRE, Procedimentos, Alertas, Gráficos, and Manual de Operação. The main content area is divided into three sections, each displaying a security alert with its details and description.

São Paulo, 06 de Abril de 2003

Acesso ao SIRE
Login: mcesar
Senha: ***
Login
Quero me cadastrar!
Esqueci minha senha!

Boletim de Segurança
E-mail: _____
Cadastrar
Descadastrar
Enviar

Últimos Alertas
Remote Buffer Overflow in Sendmail
WORM_LOVGATE.C
MS-SQL Server Worm

Alerta: Remote Buffer Overflow in Sendmail
Data: 2003-03-06
Hora: 16:50:07
Tipo: Vulnerabilidade
Nível: Crítico
Mail: [Sim](#)
Descrição:
Researchers at Internet Security Systems (ISS) have discovered a remotely exploitable vulnerability in sendmail. This vulnerability could allow an intruder to gain control of a vulnerable sendmail server.
Most organizations have a variety of mail transfer agents (MTAs) at various locations within their network, with at least one exposed to the Internet. Since sendmail is the most popular MTA, most medium-sized to large organizations are likely to have at least one vulnerable sendmail server. In
Link: <http://www.cert.org/advisories/CA-2003-07.html>

Alerta: WORM_LOVGATE.C
Data: 2003-02-24
Hora: 08:25:22
Tipo: Worm
Nível: Crítico
Mail: [Sim](#)
Descrição:
This malware is currently rapidly spreading in Taiwan, Australia, France, and Japan from where TrendLabs has received a significant number of infection reports. As of 1:02 AM, Trend has declared a Yellow Alert to control the spread of this malware.
This worm effectively uses a relatively new social engineering trick by mimicking an autoreply message where it attaches itself. Recipients are enticed into opening the malware attachment since the mimicked message arrives as a reply to a
Link: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?vName=WORM_LOVGATE.C

Alerta: MS-SQL Server Worm
Data: 2003-02-24
Hora: 07:35:41
Tipo: Worm
Nível: Crítico
Mail: [Sim](#)
Descrição:
The worm targeting SQL Server computers is self-propagating malicious code that exploits the vulnerability described in VU#484891 (CAN-2002-0649). This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow.
Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 376-bytes and send them

Estatísticas

São Paulo,
06 de Abril de 2003

Acesso ao SIRT

Login:

Senha:

[Quero me cadastrar!](#)

[Esqueci minha senha!](#)

Boletim de Segurança

E-mail:

Cadastrar

Descadastrar

Últimos Alertas

- XYZ WORM
- Remote Buffer Overflow in Sendmail
- WORM_LOVGATE.C
- MS-SQL Server Worm

USP Universidade de São Paulo BRASIL

CSIRT - Computer Security Incident Response Team

Sobre o SIRT	Boletim de Alertas	Alertas
Conheça mais sobre o projeto SIRT.	Boletim destinados aos administradores de sistemas da USP, cadastre-se já.	Últimos alertas segurança.

Procedimentos	Gráficos	Manual de Operação
Procedimentos para o dia-a-dia dos administradores de sistemas.	Gráficos dos reports recebidos pela USP nos últimos meses.	Manual de operação do sistema.

Estatísticas Personalizadas

The screenshot displays a web application interface with a navigation menu at the top: Home, Sobre o SIRC, Procedimentos, Alertas, Gráficos, and Manual de Operação. The main content area is titled "Dados de Incidentes" and contains six tables, each representing a different unit. Each table has columns for "Unidade", "Em Aberto", "Encerrado", and "Total".

On the left side, there is a sidebar with the following sections:

- São Paulo, 06 de Abril de 2003**
- Acesso ao SIRC**
 - Login: mcesar
 - Senha: ***
 - Login button
 - [Quero me cadastrar!](#)
 - [Esqueci minha senha!](#)
- Boletim de Segurança**
 - E-mail: [input field]
 - Cadastrar
 - Descadastrar
 - Enviar button
- Últimos Alertas**
 - Remote Buffer Overflow in Sendmail
 - WORM_LOVGATE.C
 - MS-SQL Server Worm

The incident data tables are as follows:

Unidade	Em Aberto	Encerrado	Total
CIAGRI	0	1	1

Tipo de Incidente	Em Aberto	Encerrados	Total
Scan	0	1	1

Unidade	Em Aberto	Encerrado	Total
CIRP	1	0	1

Tipo de Incidente	Em Aberto	Encerrados	Total
Mau Uso	1	0	1

Unidade	Em Aberto	Encerrado	Total
POLI	1	0	1

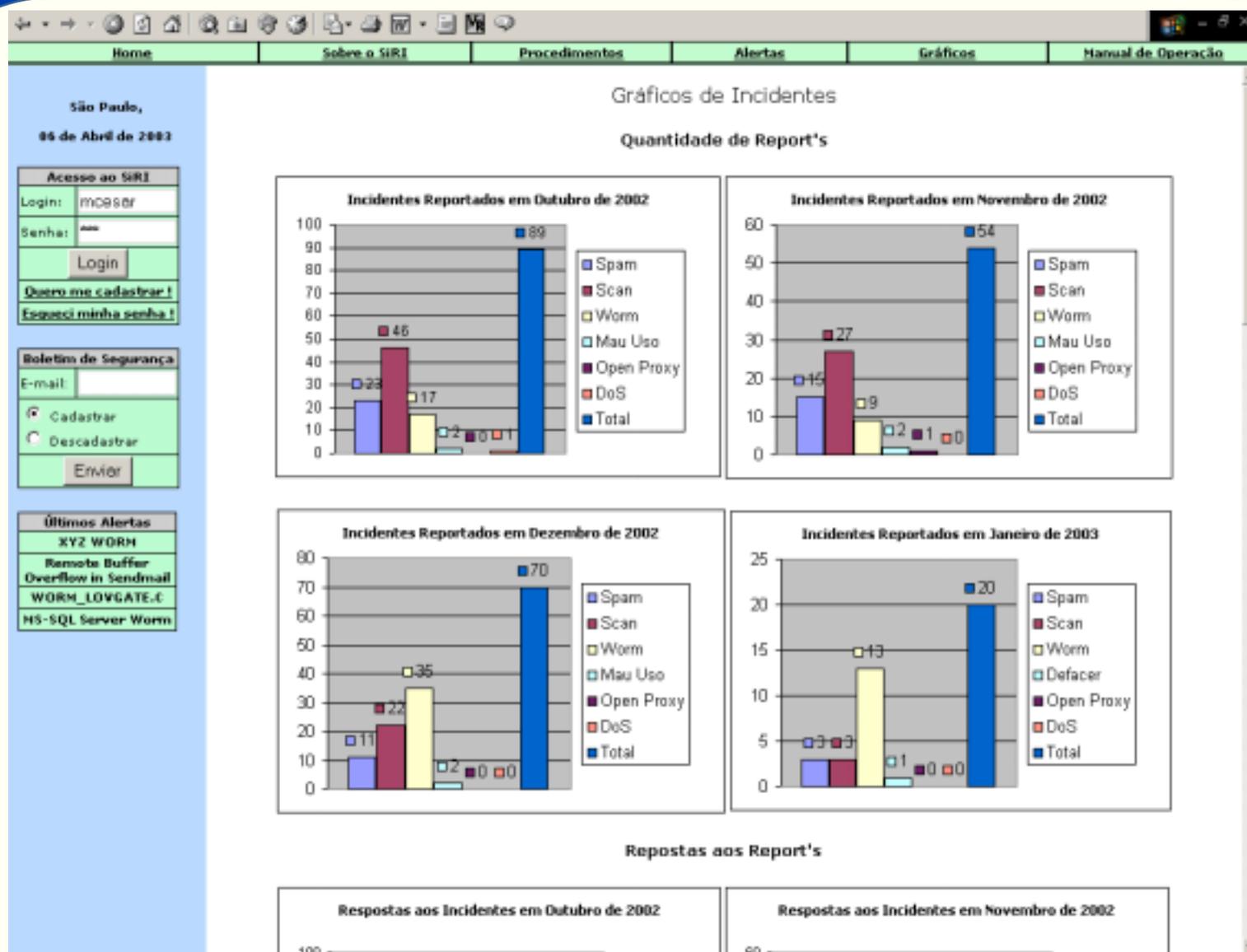
Tipo de Incidente	Em Aberto	Encerrados	Total
Spam	1	0	1

Unidade	Em Aberto	Encerrado	Total
IQ	1	0	1

Tipo de Incidente	Em Aberto	Encerrados	Total
Spam	1	0	1

Unidade	Em Aberto	Encerrado	Total
CCE	1	0	1

Gráficos Personalizados



Estadísticas

- **O fator Psicológico;**
- **Repositório de Informações;**
- **Ajuda a redefinir requisitos de controle para a Política de Segurança.**

Manual de Documentação

São Paulo,
06 de Abril de 2003

Centro de Computação Eletrônica
Universidade de São Paulo

Manual de Operação do SIRS (Sistema de Resposta a Incidentes)

Informações do Sistema

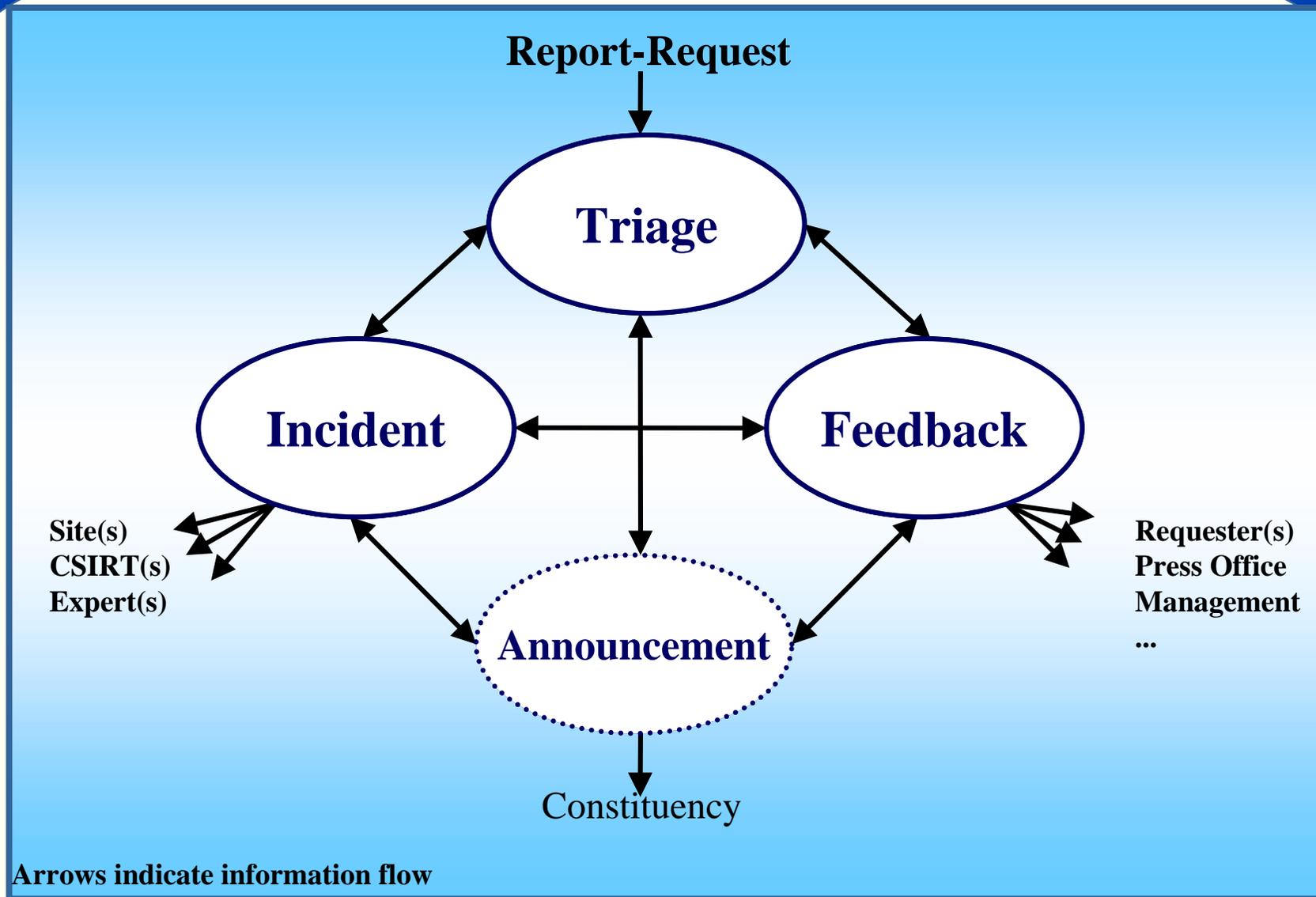
- [1.1 Cadastro de Login](#)
- [1.2 Opções do Sistema](#)
- [1.3 Cadastro do Incidente](#)
 - [1.3.1 Mensagem padrão para os administradores](#)
 - [1.3.2 Mensagem padrão em português para o reclamante](#)
 - [1.3.3 Mensagem padrão em inglês para o reclamante](#)
 - [1.3.4 Mensagem padrão para o administrador quando o incidente for encerrado](#)
 - [1.3.5 Mensagem padrão em inglês para o reclamante quando o incidente for encerrado](#)
 - [1.3.6 Mensagem padrão, em português, para o reclamante](#)
 - [1.3.7 Mensagem padrão para o administrador](#)
 - [1.3.8 Dados do Incidente Cadastrado](#)
- [1.4 Consultas de Incidentes](#)
- [1.5 Alteração de Incidentes](#)
- [1.6 Alteração de Status do Incidente](#)
- [1.7 Acompanhamento de Incidente](#)
- [1.8 Dados de Incidentes](#)
- [1.9 Incidentes em situação crítica](#)
- [1.10 Gráficos](#)

1.0 Informações do Sistema
O projeto do SIRS (Sistema de Resposta a Incidentes) do Centro de Computação e Eletrônica da Universidade de São Paulo teve início em Outubro de 2002, a partir de uma iniciativa da equipe de segurança de

O Cenário Atual

- **Redução de 60% do tempo despendido no ciclo de vida de uma Resposta a Incidentes;**
- **Acompanhamento personalizado de cada incidente;**
- **Maior interação entre o reclamante, a equipe de segurança e os administradores responsáveis;**
- **Constituição de um Repositório de Informações.**
- **Ferramenta auxiliar para as etapas previstas para a atividade de Resposta a Incidentes;**

IR Service Functions Overview



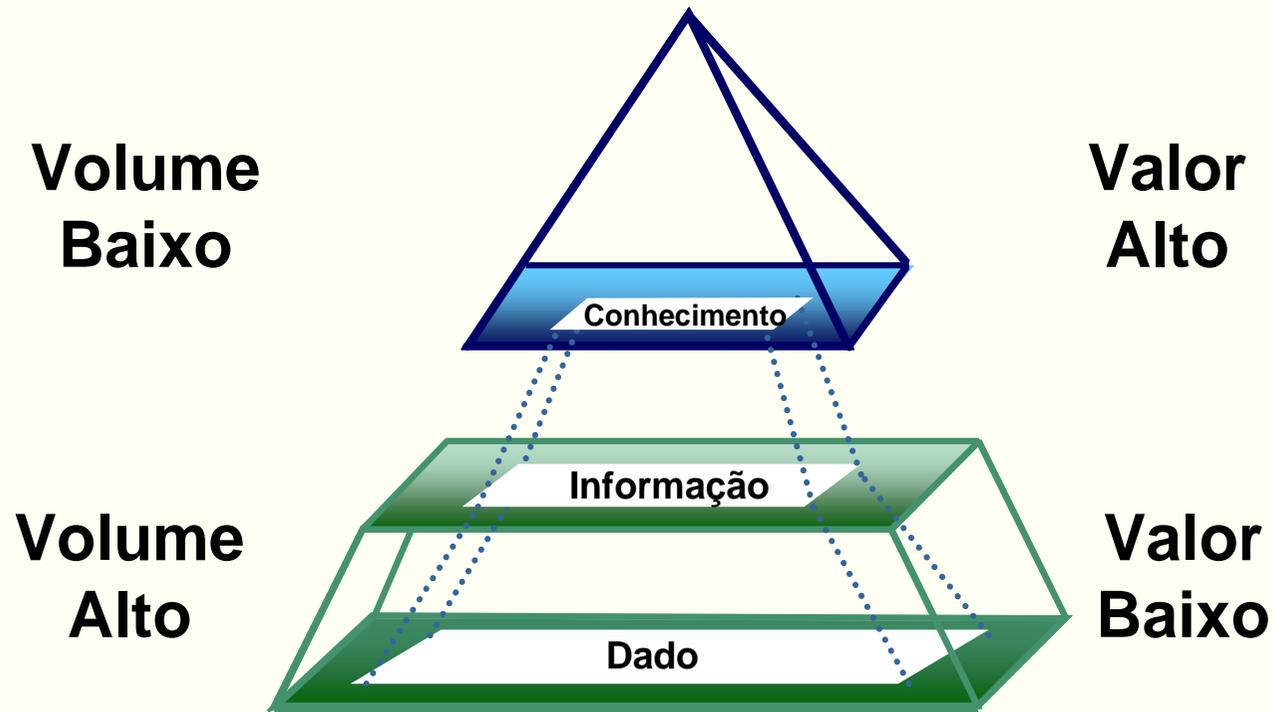
Fonte: <http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>

Trabalhos Futuros

Constituição de um Sistema de Informações

- Trabalhar dados para produzir informação e conhecimento;
- Fornecer suporte à tomada de decisão;
- **Expectativa:** Um sistema integrado homem-máquina que provê informações para dar suporte às funções de operação, administração e tomada de decisão em relação à segurança computacional;
- Código aberto a contribuições.

Metodologia: Dados, Informação e Conhecimento



Aquisição de conhecimento (AC):
Extração, interpretação e representação
do conhecimento de um dado domínio.
Tarefa difícil!

Sistemas de Informação e Estrutura de Decisão



Classificação dos Sistemas de Informação



Extração de conhecimento de Base de Dados

Objetivos:

Apoiar os especialistas do domínio na obtenção de conhecimento de base de dados;

KDD (Knowledge Discovery in Databases)

KDD

(Knowledge
Discovery
in Databases)

Elementos de Apoio ao Processo KDD

- *Data Warehouse;*
- **Técnicas Estatísticas;**
- **Visualização de Dados**

Expectativa

Utilização dos conceitos de sistemas de informação para modelar um ambiente que permita ao administrador de segurança computacional, metodicamente, gerar conhecimento para planejar e programar a tomada de decisão com a eficiência e a eficácia exigidas pelos sistemas/redes atuais.

Conclusões

- **A ferramenta apresentada apresentou contribuições significativas no processo de RI;**
- **Entretanto, a ferramenta SiRI é apenas o início de um projeto para a constituição de um sistema de informação;**
- **Trabalho colaborativo é essencial!**