



**2ª Oficina de Segurança da
Informação e Comunicações
(SIC) de 2016**



Objetivo

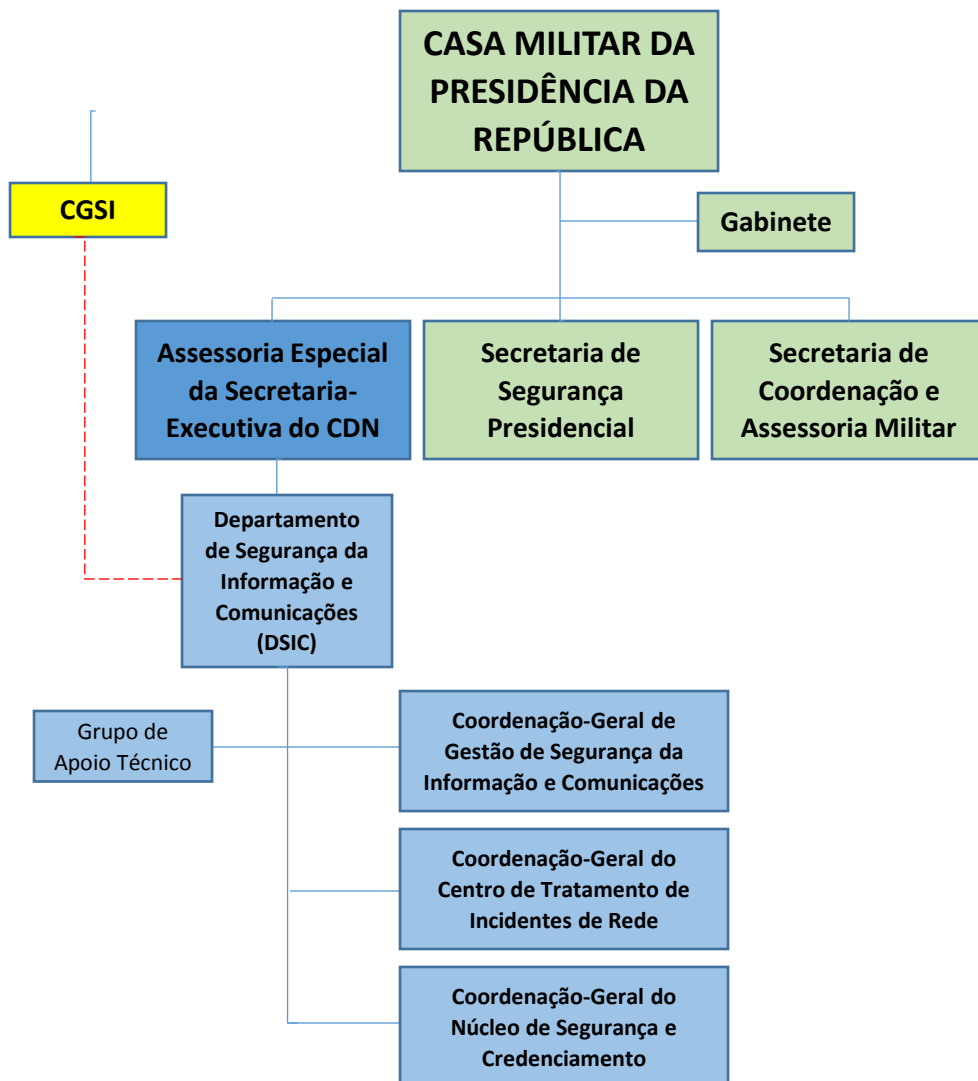


Apresentar as normas NC05/IN01/DSIC/GSIPR (Criação de ETIRs) e NC08/IN01/DSIC/GSIPR (Tratamento de Incidentes de Redes na APF).

Apresentar o CTIR Gov, sua missão Institucional, metodologia, ferramentas, estudos de caso e os desafios éticos para ETIRs.



Estrutura – DSIC



Portaria 25/2015 do SE/CDN (Aprova o Regimento Interno do CGSI)

[...]

Art. 6º **O Diretor do** Departamento de Segurança da Informação e Comunicações **(DSIC)** do GSI/PR, representante titular deste Gabinete, **exercerá as atribuições de Coordenador do CGSI.**



Introdução



(Art. 2º - IN01/DSIC/GSIPR)





Introdução



Segurança da Informação e Comunicações (SIC)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.



Introdução



Segurança da Informação e Comunicações (SIC)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;



Introdução



Segurança da Informação e Comunicações (SIC)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;



Introdução



Segurança da Informação e Comunicações (SIC)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e Credenciado;



Introdução



Segurança da Informação e Comunicações (SIC)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e Credenciado;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;



Introdução



Segurança da Informação e Comunicações (SIC)

(Art. 2º - IN01/DSIC/GSIPR)

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**, e o **Não Repúdio** das Informações.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e Credenciado;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Não Repúdio: ou não recusa, é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital.



Arcabouço Normativo - DSIC



Instrução Normativa nº 1 de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

NC 01/2008	Atividade de Normatização .
NC 02/2008	Metodologia de Gestão de SIC.
NC 03/2009	Diretrizes para a Elaboração de Política de SIC.
NC 04/2013	Diretrizes para o processo de Gestão de Riscos de SIC - GRSIC. (Revisão 01)
NC 05/2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR .
NC 06/2009	Estabelece Diretrizes para Gestão de Continuidade de Negócios , nos aspectos relacionados à SIC.
NC 07/2014	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à SIC.
NC 08/2010	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais .
NC 09/2014	Estabelece orientações específicas para o uso de recursos criptográficos em SIC. (Revisão 02)
NC 10/2012	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação , para apoiar a SIC.
NC 11/2012	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à SIC.
NC 12/2012	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC.
NC 13/2012	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à SIC.
NC 14/2012	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem , nos aspectos relacionados à SIC.
NC 15/2012	Estabelece diretrizes de SIC para o uso de redes sociais .
NC 16/2012	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro .
NC 17/2013	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de SIC.
NC 18/2013	Estabelece as Diretrizes para as Atividades de Ensino em SIC.
NC 19/2014	Estabelece Padrões Mínimos de SIC para os Sistemas Estruturantes da APF.
NC 20/2014	Estabelece as Diretrizes de SIC para Instituição do Processo de Tratamento da Informação . (Revisão 01)
NC 21/2014	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da APF.



Instrução Normativa GSI/PR Nº 1



Art. 1º - Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

Art. 3º - por intermédio do **Departamento de Segurança da Informação e Comunicações - DSIC**, compete:
III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

Art. 5º - Aos **demais órgãos e entidades da Administração Pública Federal, direta e indireta**, em seu âmbito de atuação, compete:

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

Art. 7º - Ao **Gestor de Segurança da Informação e Comunicações**, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;



NC 05/2009 – Criação de ETIRs



OBJETIVO: Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2.4- É competência da **Coordenação-Geral de Tratamento de Incidentes de Redes** do Departamento de Segurança da Informação e Comunicações – DSIC do Gabinete de Segurança Institucional – GSI apoiar os órgãos e entidades da Administração Pública Federal, direta e indireta, nas atividades de capacitação e tratamento de incidentes de segurança em redes de computadores, conforme disposto nos incisos III e VI do art. 39 do anexo da Portaria nº 13 do GSI, de 04 de agosto de 2006.

4.1- Agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

5- Responsabilidade: Os Gestores de Segurança da Informação e Comunicações são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, nos órgãos e entidades da Administração Pública Federal, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.



NC 05/2009 – Criação de ETIRs



7- MODELOS DE IMPLEMENTAÇÃO:

7.1 Modelo 1 – **Utilizando a equipe de Tecnologia da Informação – TI**

Não existirá um grupo dedicado, age reativamente, Agente Responsável atribui responsabilidades para que os seus membros exerçam atividades pró-ativas.

7.2 Modelo 2 – **Centralizado**

Centralizada no âmbito da organização, pessoal com dedicação exclusiva.

7.3 Modelo 3 – **Descentralizado**

ETIRs distribuídas por diversos locais dispersos fisicamente dentro da organização, e chefiada pelo Agente Responsável designado.

7.4 Modelo 4 – **Combinado ou Misto**

Junção dos modelos Descentralizado e Centralizado, Equipe Central e Equipes distribuídas pela organização, Equipe central responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas.



NC 05/2009 – Criação de ETIRs



8-ESTRUTURA ORGANIZACIONAL:

8.1- Existem muitas maneiras diferentes de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ser estruturada. A estrutura dependerá do modelo de implementação a ser adotado, do tamanho da organização, do número de localizações geográficas distribuídas e onde as funções estão localizadas, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos e do conhecimento técnico do pessoal existente.

8.2- Os membros da Equipe deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede, os quais deverão dedicar o tempo integral, ou um percentual do seu tempo de trabalho, dependendo do modelo de implementação adotado, de forma reativa e pró-ativa.

8.4- Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. A Equipe poderá ser estendida com a inclusão dos seguintes membros: representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado.



NC 05/2009 – Criação de ETIRs



9- AUTONOMIA DA ETIR:

9.1 Autonomia Completa

Tem plena autonomia, conduz o seu público alvo para realizar ações necessárias na recuperação de incidentes de segurança, Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

9.2 Autonomia Compartilhada

ETIR possui a autonomia compartilhada, trabalha em acordo com os outros setores no processo de tomada de decisão sobre quais medidas devam ser adotadas. A indicação dos membros do processo decisório deverá ser definida explicitamente no documento de constituição da ETIR.

9.3 Sem Autonomia

ETIR não terá autonomia para a tomada de decisões ou adoção de ações, podendo, no entanto, recomendar os procedimentos a serem executados, mas não terá um voto na decisão final.



NC 05/2009 – Criação de ETIRs



10- DISPOSIÇÕES GERAIS:

10.2 Preferencialmente a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos.

10.3 Cada órgão poderá deliberar o nome de sua Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

10.4 A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

10.5 A ETIR poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar.

10.6 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao **CTIR GOV**, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.



NC 05/2009 – Criação de ETIRs



ANEXO A

DOCUMENTO DE CONSTITUIÇÃO DA ETIR:

MISSÃO

COMUNIDADE OU PÚBLICO ALVO

MODELO DE IMPLEMENTAÇÃO

ESTRUTURA ORGANIZACIONAL

AUTONOMIA DA ETIR

SERVIÇOS



NC 05/2009 – Criação de ETIRs



BOLETIM DE PESSOAL E SERVIÇO

Brasília, 25 de março de 2011 ISSN 1519-9037 Ano 42 - Número 3.16 - ESPECIAL

Sumário	
SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO	1
SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO	1

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO

PORTARIAS SLTI DE 25 DE MARÇO DE 2011

NP 13 -
Institui a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais - ETIR, no âmbito do Ministério do Planejamento, Orçamento e Gestão.

O GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, no uso da competência que lhe confere a Portaria nº 56, de 23 de fevereiro de 2011, o disposto no Decreto nº 3.525, de 13 de junho de 2000, no Decreto nº 4.553, de 27 de dezembro de 2002, na Norma Complementar nº 425, de 14 de agosto de 2009 e na Instrução Normativa nº 1, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2009, resolve:

Art. 14 Institui o Centro de Tratamento e Resposta a Ataques na Rede MP – Cetra, no âmbito do Ministério do Planejamento, Orçamento e Gestão, vinculado ao Departamento Setorial de Tecnologia da Informação e Tecnologia da Informação – DSTI/SLTI, observadas as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações e pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 24 O Centro de Tratamento e Resposta a Ataques na Rede MP – Cetra será a Equipe de Tratamento em Incidentes de Redes Computacionais – ETIR do Ministério do Planejamento.

Art. 34 O Cetra tem por missão: “Garantir a Segurança da Informação e Comunicações no âmbito do Ministério do Planejamento, por meio do efetivo cumprimento da Política de Segurança, suas normas e da gestão de riscos contínuas”.

Art. 40 O Cetra tem como atribuições:

- I – Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais;
- II – Promover a recuperação de sistemas;
- III – Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança e, avaliando condições de segurança de redes por meio de auditorias;
- IV – Realizar ações relativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsabilidades;
- V – Analisar ataques e intrusões na rede MP;
- VI – Estabelecer regras para ações disciplinares no caso de condutas que violem as políticas estabelecidas ou que comprometam a segurança das informações de organização;
- VII – Cooperar com outras equipes de Tratamento e Resposta a Incidentes Computacionais, e
- IX – Participar em fóruns, redes nacionais e internacionais.

Art. 54 As proposições de que trata o art. 24 desta Portaria serão submetidas ao Comitê de Segurança da Informação e Comunicações – CSIC do Ministério.

Art. 56 A ETIR Cetra adotará o modelo de implementação combinado ou misto onde existirá uma ETIR central (Cetra) e equipes descentralizadas no âmbito do Ministério do Planejamento, supervisionadas pela ETIR Cetra.

Art. 74 O agente responsável pela ETIR será designado por meio de Portaria própria.

Art. 84 A ETIR Cetra será composta por membros da Coordenação de Suporte Tecnológico, da Coordenação-Cetra e Tecnologia da Informação, do Departamento Setorial de Tecnologia da Informação, da Secretaria de Logística e Tecnologia da Informação – DSTI/SLTI e coordenação e o apoio administrativo necessários ao funcionamento da ETIR Cetra.

Art. 94 As demais unidades administrativas do Ministério serão convidadas a indicar membros para compor a ETIR Cetra, desde que devidamente treinados e orientados e, comprovados conhecimentos específicos na área de Segurança da Informação e Comunicações.

Art. 10 A Equipe Cetra propõe ao Comitê de Segurança da Informação, no prazo máximo de 30 dias de sua constituição, o regimento interno da ETIR e a designação dos seus membros.

Parágrafo único. Para cada membro da ETIR Cetra deverá ser designado um substituto devidamente treinado e orientado para a realização das tarefas e atividades da ETIR.

Art. 11 Caberá ao Departamento Setorial de Tecnologia da Informação da Secretaria de Logística e Tecnologia da Informação – DSTI/SLTI a coordenação e o apoio administrativo necessários ao funcionamento da ETIR Cetra.

Art. 12 Esta Portaria entra em vigor na data de sua publicação.

NP 14 -
Institui o Agente Responsável pelo Centro de Tratamento e Resposta a Ataques na Rede MP – Cetra, no âmbito do Ministério do Planejamento, Orçamento e Gestão.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

O GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, no uso da competência, resolve:

Art. 1º Instituir o Centro de Tratamento e Resposta a Ataques na Rede MP – Cetra, no âmbito do Ministério do Planejamento, Orçamento e Gestão, vinculado ao Departamento Setorial de Tecnologia da Informação da Secretaria de Logística e Tecnologia da Informação - DSTI/SLTI, observadas as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações e pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR.

Art. 4º O Cetra tem como **atribuições**:

I – Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais

Art. 6º A ETIR Cetra adotará o **modelo de implementação combinado ou misto**

Art. 8º A ETIR Cetra será composta **por membros da – COTEC/CGTI/DSTI/SLTI.**

Atribuir ao Agente Responsável pelo Centro de Tratamento e Resposta a Ataques na Rede MP - Cetra as seguintes competências:

IX - Assistir o CTIR GOV com as informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal;



Criação de ETIRs



RELATO DE EXPERIÊNCIAS

- Pontos Positivos
- Pontos Negativos
- Tempo Envolvido
- Quantidade de Pessoas
- Custo
- Serviços Oferecidos
- Ferramentas



NC 08/2010 – Incidentes em Redes Computacionais



1- OBJETIVO:

Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

5- RESPONSABILIDADE:

O Agente Responsável, designado no documento de criação da ETIR, é o responsável pela ETIR do seu órgão ou entidade, bem como pelo relacionamento com o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov.

6- RELACIONAMENTOS DA ETIR:

A ETIR comunicará a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.



NC 08/2010 – Incidentes em Redes Computacionais



7.1- Recomenda-se que a ETIR defina os serviços a serem oferecidos à sua comunidade e, na medida em que forem oferecidos, que o sejam de forma gradativa e de acordo com a maturidade da equipe;

7.2- Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores:

7.2.1- Tratamento de artefatos maliciosos;

7.2.2- Tratamento de vulnerabilidades;

7.2.3- Emissão de alertas e advertências;

7.2.4- Anúncios;

7.2.5- Prospecção ou monitoração de novas tecnologias;

7.2.6- Avaliação de segurança;

7.2.7- Desenvolvimento de ferramentas de segurança;

7.2.8- Detecção de intrusão;

7.2.9- Disseminação de informações relacionadas à segurança;



Ambientação – CTIR Gov



Coordenação-Geral de Tratamento de Incidentes de Redes

✓ Missão (Art.39 Port. nº 13, de agosto/2006)

- (...) **operar e manter o Centro de Tratamento de Incidentes de Redes de Computadores da Administração Pública Federal;**
- **apoiar** *órgãos e entidades da Administração Pública Federal nas atividades de tratamento de Incidentes de Segurança de Redes de computadores;*
- **monitorar e analisar** *tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal; (...)*

✓ Centro de Coordenação Nacional

O CTIR Gov age como **centro de coordenação de responsabilidade nacional**, na ligação entre os envolvidos e no acompanhamento das ações de tratamento e resposta aos incidentes de segurança ocorridos na APF.

✓ Comunidade de Tratamento de Incidentes do CTIR Gov

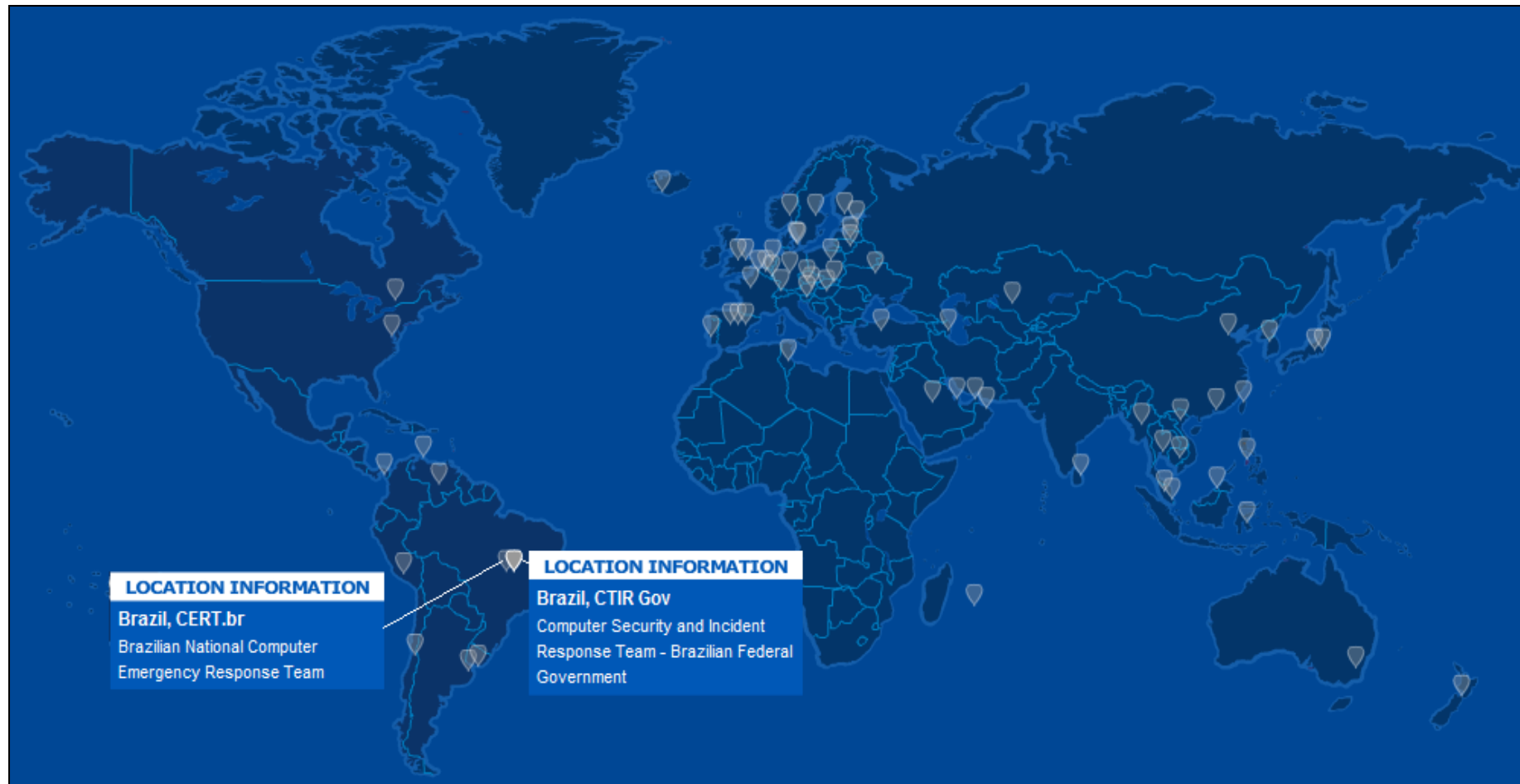
Composta por todos os órgãos e entidades da APF direta e indireta. Em caráter excepcional e de forma colaborativa os órgãos dos Estados e Municípios, pertencentes aos domínios “**gov.br**”, “**jus.br**”, “**leg.br**”, “**mil.br**”, “**mp.br**” e outros.



Ambientação – CTIR Gov



Centros de Tratamento de Incidentes com Responsabilidade Nacional



Fonte: <http://www.cert.org/csirts/national/>



Linha do Tempo – CTIR Gov



2016	Melhoria dos processos automatizados visando obter melhor performance, e atualizar a documentação dos processos existentes (em andamento).
2014	Implantação do Data WareHouse de Incidentes integrado ao Sistema automatizado de incidentes.
2012	Aperfeiçoamento dos processos, ampliação do número de serviços oferecidos pelo CTIR Gov à APF e intensificação de trocas de informação com parceiros
2010	Implantação do RT (<i>Request Tracker</i>) como ferramenta para suportar o modelo de negócios do CTIR Gov
2008	Criação do “Modelo de melhoria de qualidade baseado em processos para tratamento de incidentes de rede na APF”
2006	Competências da CGTIR publicadas em Portaria Ministerial



Serviços / Comunidade – CTIR Gov



Serviços Realizados

Capacitação

- Estágio CDCiber;
- Criação de ETIR's;
- Colóquios técnicos.

Integração com outros atores:

- SRCC/DPF/MJ
- CERT.br/NIC.br;
- CAIS/RNP;
- CDCiber/MD;
- FEBRABAN.

Atuação em Grandes Eventos

- Rio+20;
- Copa das Confederações;
- Jornada Mundial da Juventude;
- Copa do Mundo FIFA 2014;
- Jogos Olímpicos RIO 2016.

Público-Alvo

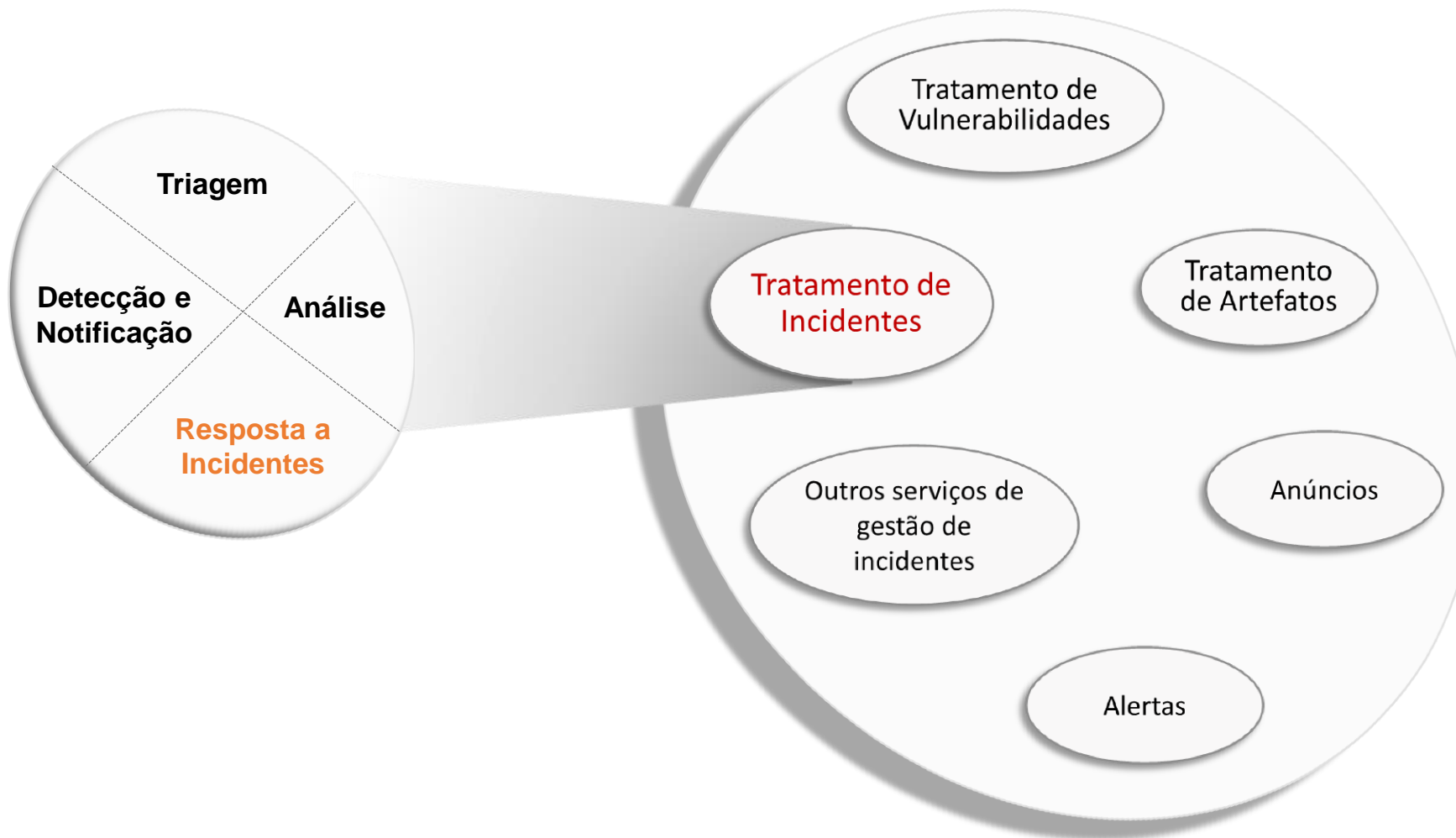
Comunidade

- Órgãos e entidades da APF (direta e indireta);
- Órgãos Estaduais e Municipais;

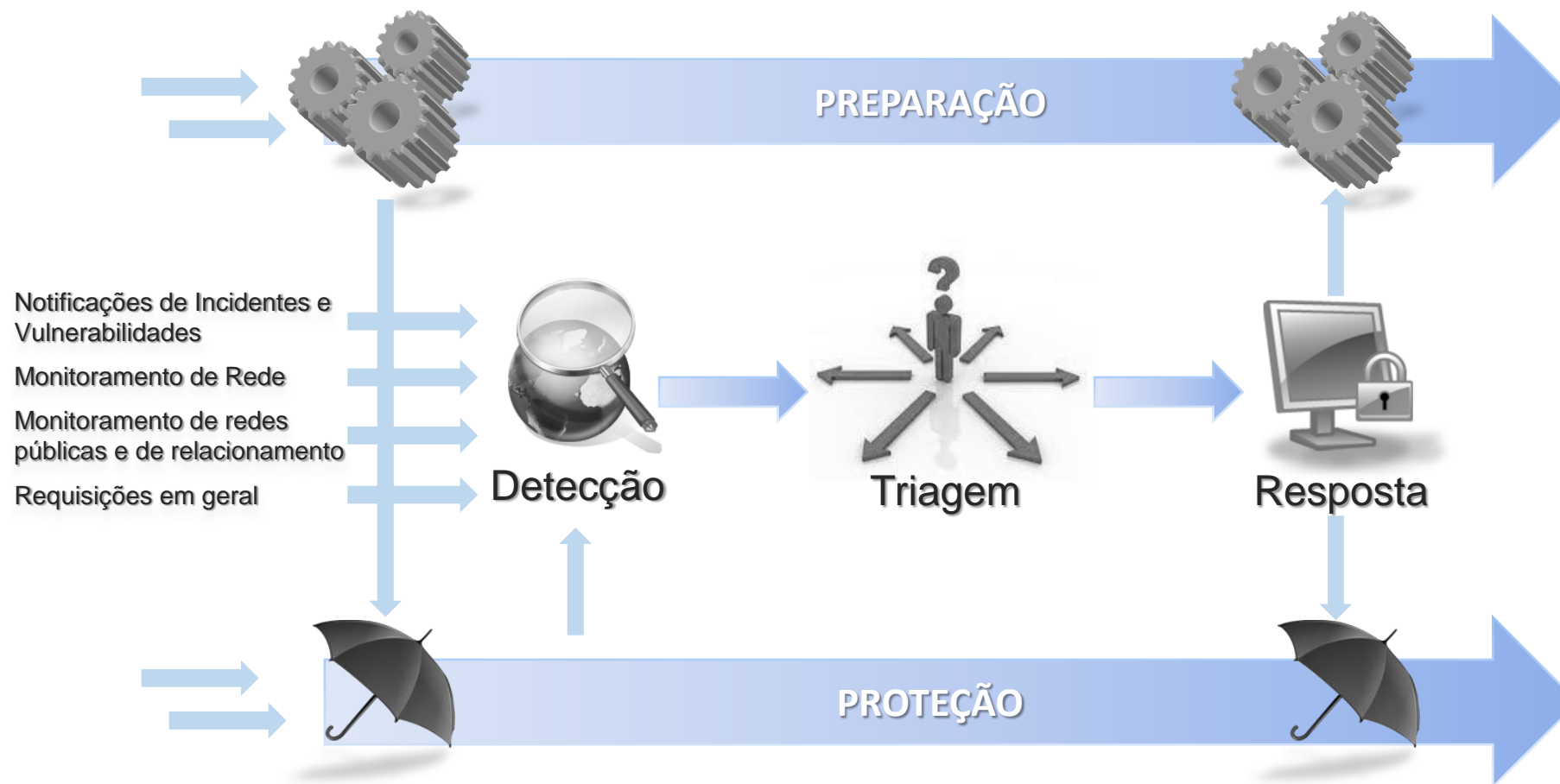
Domínios

*.gov.br, *.mil.br, *.jus.br, *.leg.br e *.mp.br

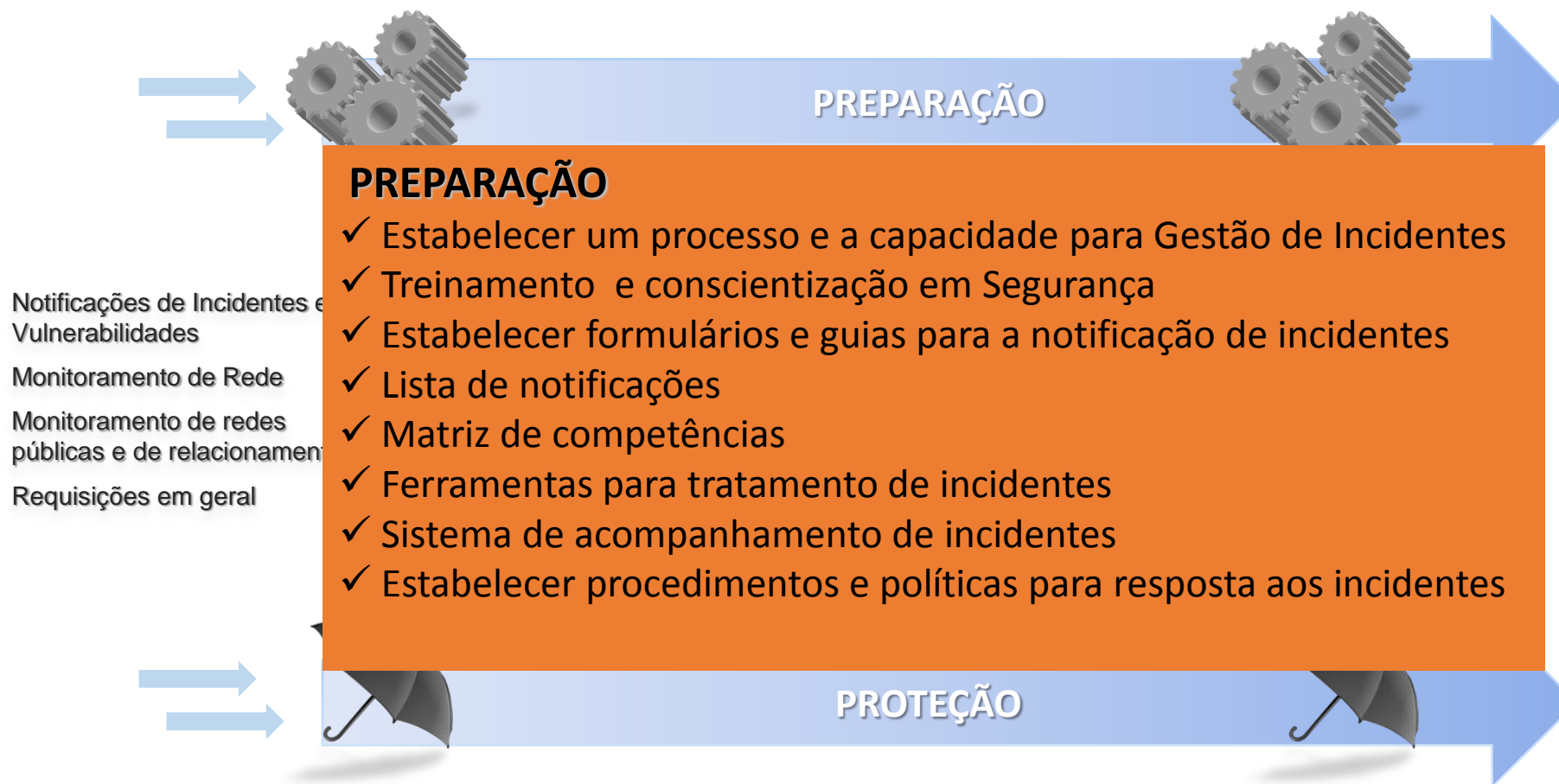
Metodologia de Gestão de Incidentes



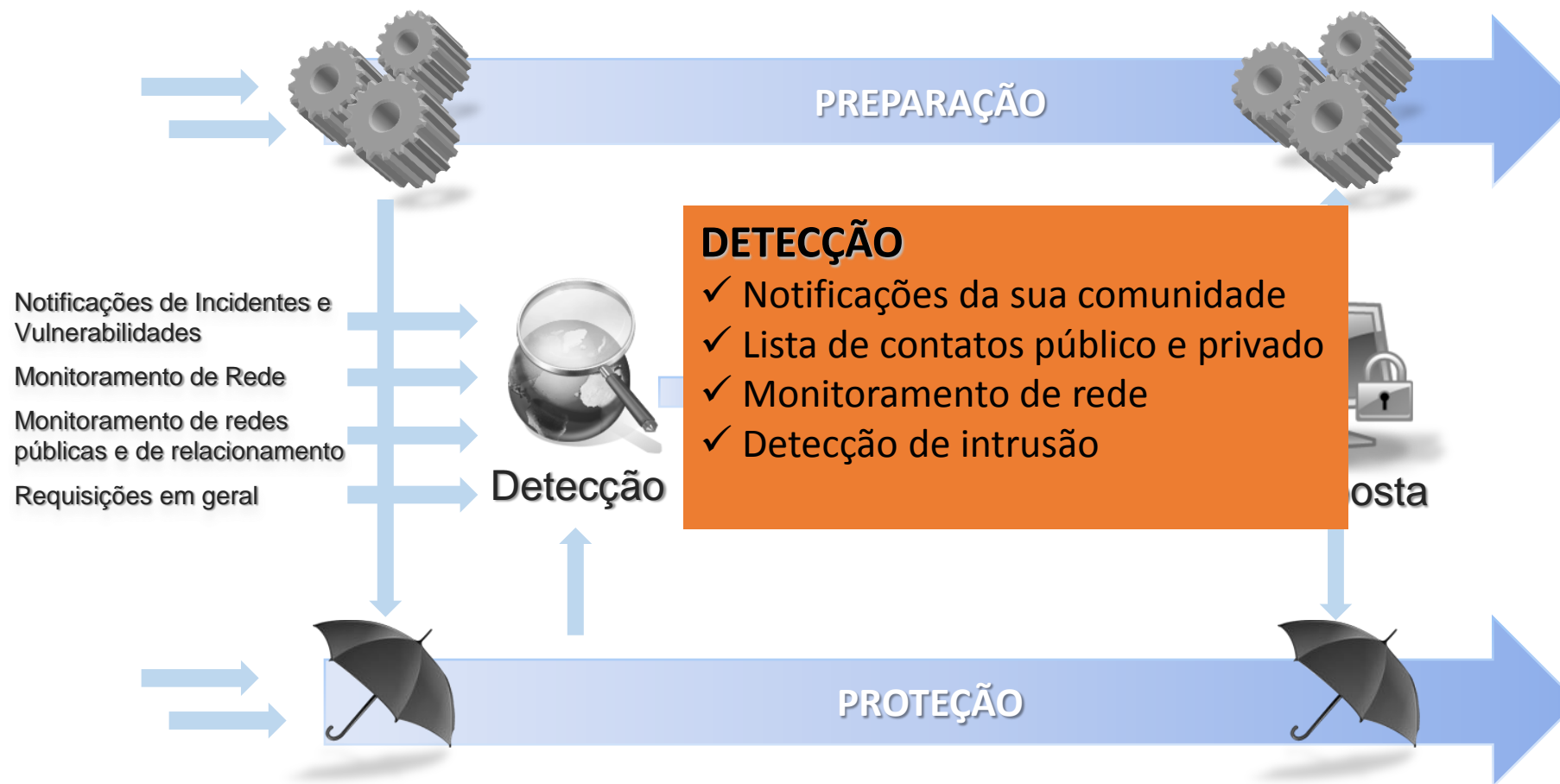
Metodologia de Gestão de Incidentes



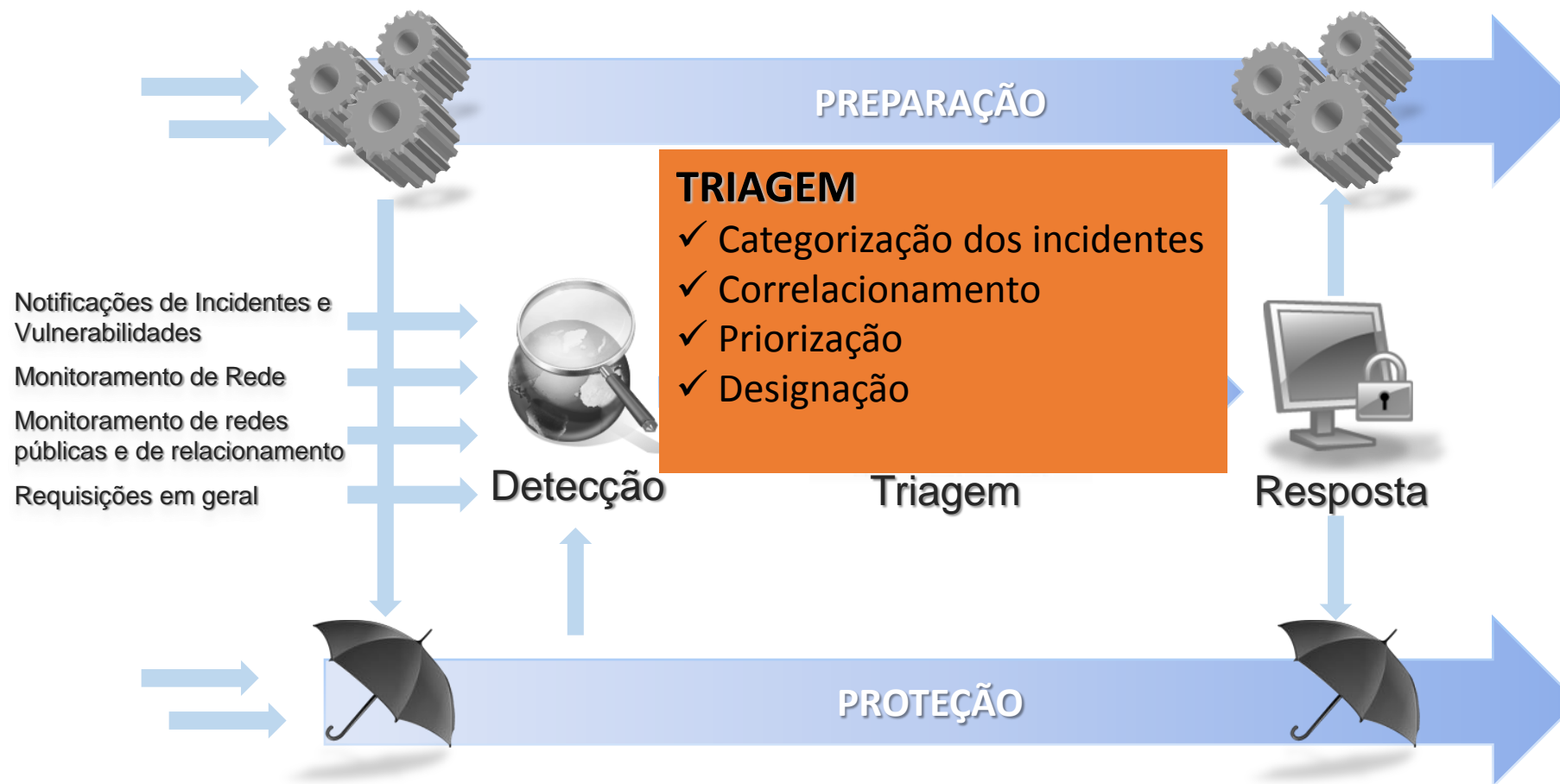
Metodologia de Gestão de Incidentes



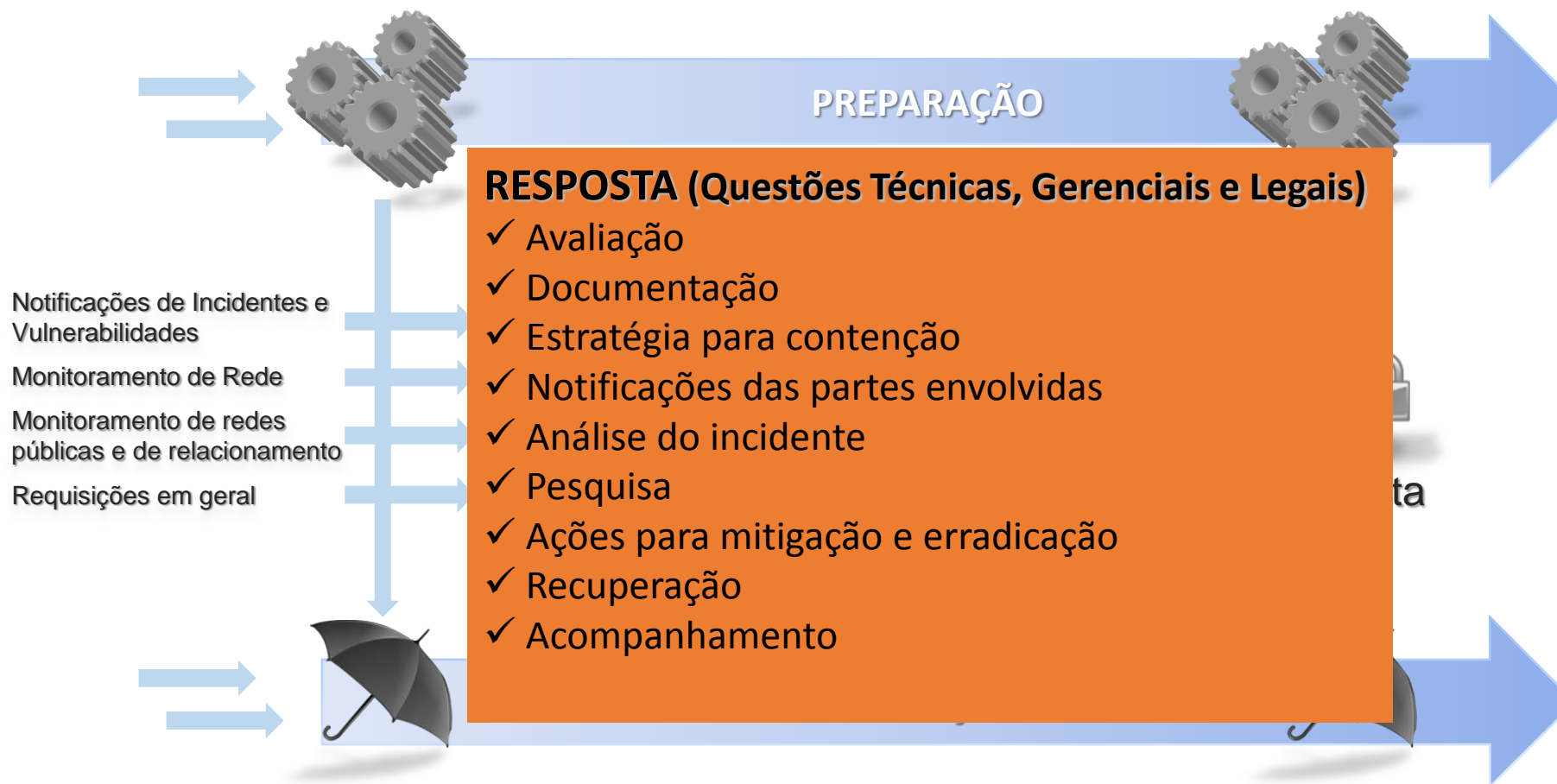
Metodologia de Gestão de Incidentes



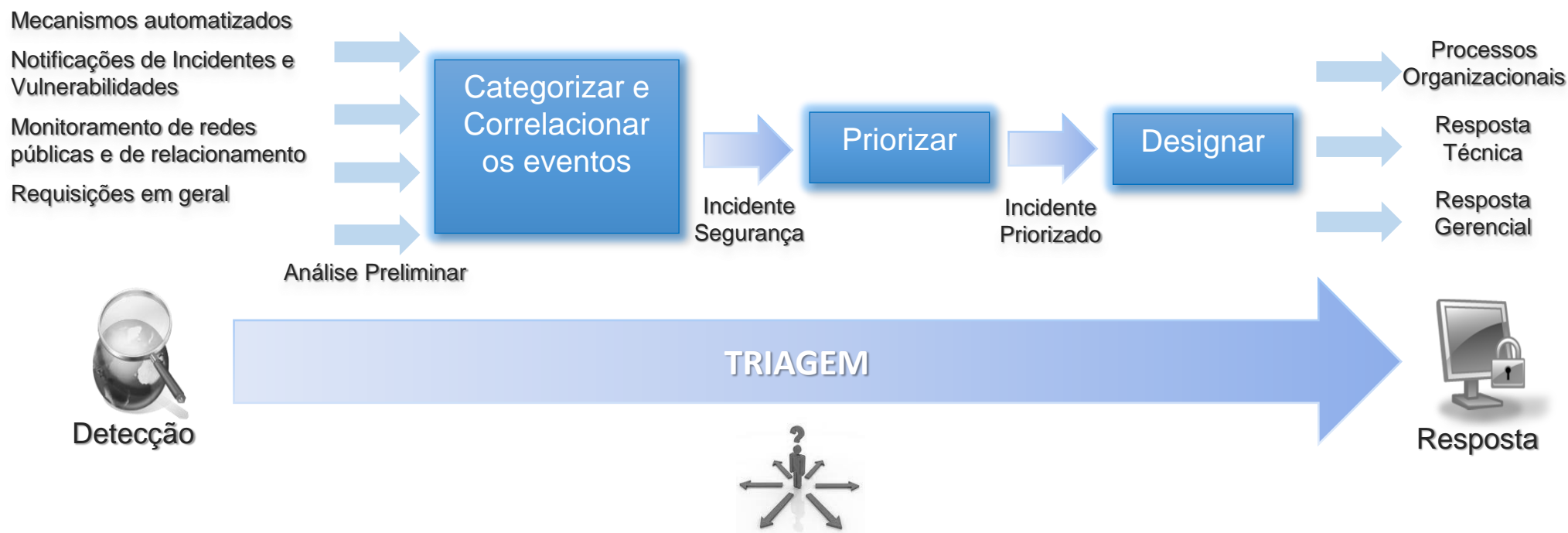
Metodologia de Gestão de Incidentes



Metodologia de Gestão de Incidentes



Metodologia de Gestão de Incidentes



Modelo de melhores práticas para Gestão de Incidentes

Fonte: Adaptado do CERT-CC



Implantação do Issue Tracking System (ITS) - Request Tracker (RT).

“Issue Tracking Systems (ITS) são sistemas destinados a controlar e registrar o andamento de cada atividade desenvolvida por uma dada equipe.”

(VINCENT et al., 2005, p.1)

Destinam-se principalmente a:

- Registrar um evento (notificação);
- Atribuir um responsável pela atividade;
- Determinar as partes envolvidas; e
- Rastrear as mudanças ocorridas.

No contexto de uma ETIR podem:

- Automatizar etapas;
- Criar modelos de notificação;
- Aumentar a produtividade; e
- Reduzir erros nas notificações.



Implantação do Issue Tracking System (ITS) - Request Tracker (RT).

BENEFÍCIOS DO RT:

➤ **Ponto de vista do usuário (analista)**

- Interface web
- Infraestrutura transparente

➤ **Ponto de vista do desenvolvedor**


- Software Livre
- Escrito em Perl
- Base de dados MySQL
- Possui interface para desenvolvimento (API) versátil
- Fóruns e comunidades atuantes
- Usado em grandes corporações como Nasa, MIT, Nike, etc.



Tratamento de Incidentes – CTIR Gov



Implantação do Issue Tracking System (ITS) - Request Tracker (RT).



HOME | [PRODUCTS](#) | SERVICES | DOCUMENTATION | LABS | JOBS | ABOUT | BLOG | SHOP

RT RT For Incident Response Assets For RT

About RT

- » Introduction
- » What's New in 4
- » Features
- » Download
- » Screenshots
- » Who uses RT
- » Praise for RT
- » Extensions
- » Languages
- » Training
- » Support
- » Managed Hosting

Technical

- » Documentation
- » Release Notes
- » Release Policy
- » Mailing Lists
- » Requirements
- » Bug Reports
- » Buy the Book
- » Version Control
- » Community Wiki


RT: Request Tracker

Who uses RT?

RT is used by thousands of organizations ranging from **Fortune 50 companies** to **government agencies**. These are just some of the trusted brands which **rely on RT** in their organization **every day**.

Compared to other products, RT is amazing and allows us to focus on helping customers and projects.

—Jeremy Hitchcock, DynDNS.com



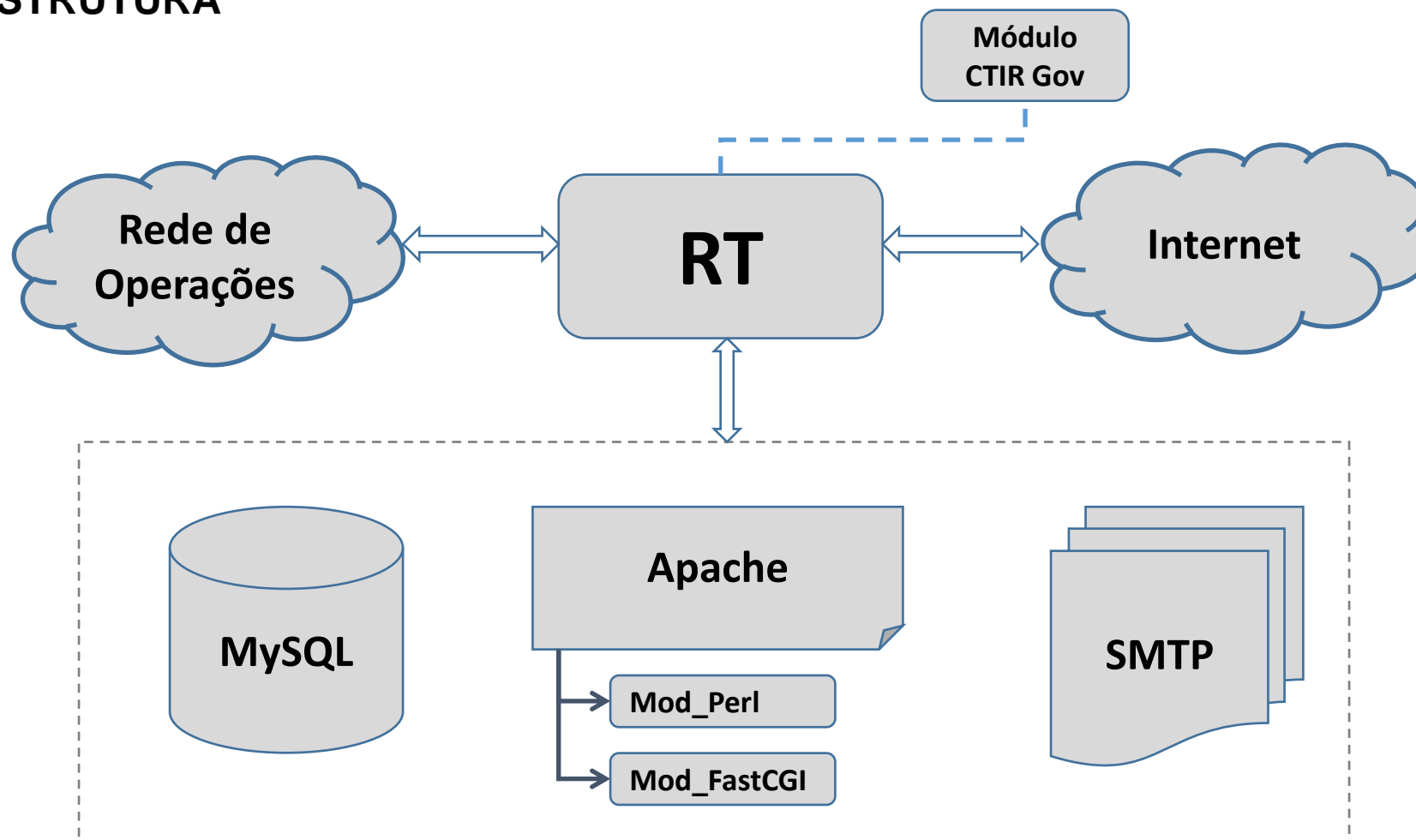


Tratamento de Incidentes – CTIR Gov

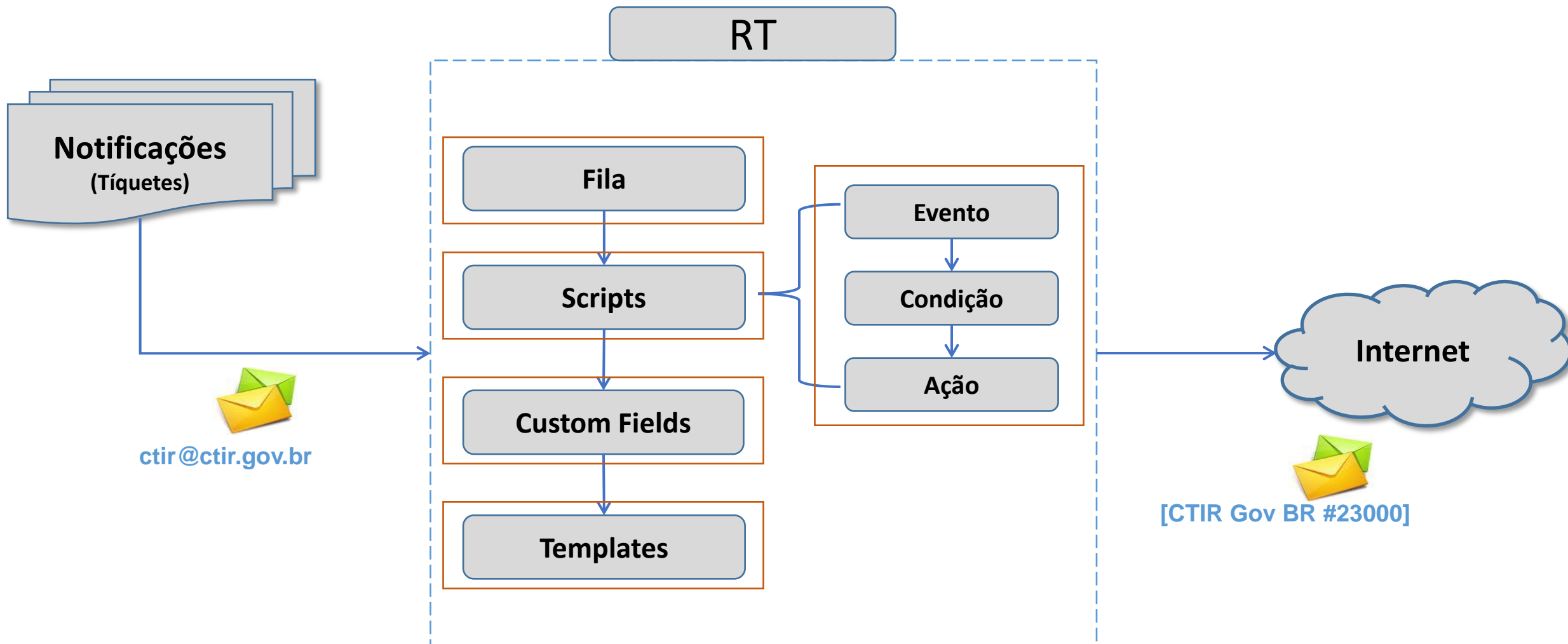


Implantação do Issue Tracking System (ITS) - Request Tracker (RT).

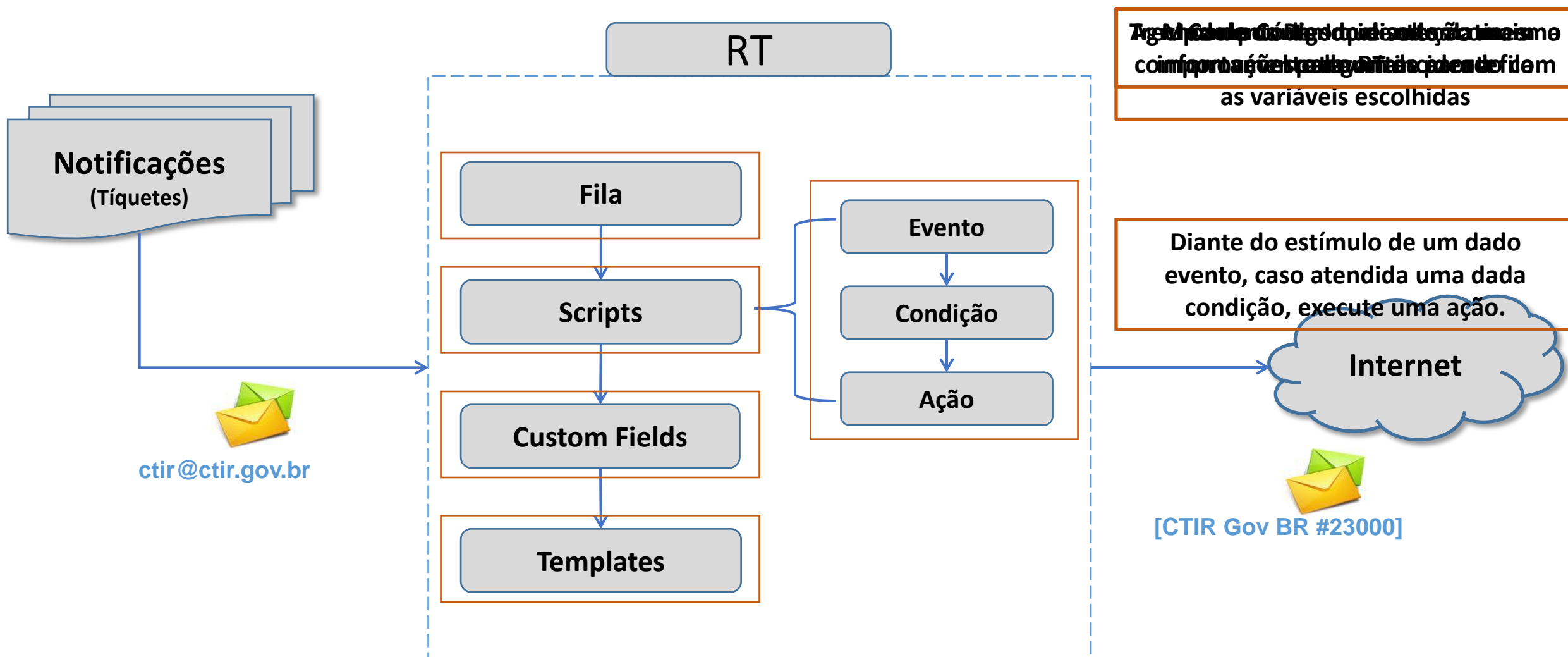
➤ INFRAESTRUTURA



Customização do Request Tracker (RT).



Customização do Request Tracker (RT).





Tratamento de Incidentes – CTIR Gov



RT para CTIR Gov BR

Entrou como charlie | Preferências | Sair

Novo ticket em Administração Buscar...

RT por alto

Página Inicial · Tickets Criados Hoje · Tickets Resolvidos Hoje · Tickets de Hoje - Analista

60 tickets de mais alta prioridade que eu possuo

#	Assunto	Prioridade	Fila	Estado
27045	Tentativas de intrusão e exploração de vulnerabilidade [136.211]	10	General	aberto

Pendentes de Charlie

#	Assunto	Estado	Fila	Proprietário	Prioridade	Atualizado em
	Requisitantes	Criado	Última atualização	Atualizado em	Tempo Restante	
27033	Malware Hosting [ks3001222.kimsufi.com]37.59.40.186]	pendente 32 horas atrás	Malware_Hosting 30 horas atrás	charlie 30 horas atrás	0	Ter Ago 28 13:54:29 2012
26951	3ª NOTIFICAÇÃO - Desfiguração de Site - Spamdexing [www.203.67]	pendente 4 dias atrás	Site_Abuse 2 dias atrás	charlie 2 dias atrás	0 4 semanas	Seg Ago 27 12:58:41 2012
26908	Malware Hosting [escenics.com]69.36.179.155]	pendente 6 dias atrás	Malware_Hosting 6 dias atrás	charlie 7 horas atrás	0	Qua Ago 29 13:22:49 2012
26899	Hospedagem de Artefato/RFI [www.dandor.com.br]186.202.153.48]	pendente 6 dias atrás	Artifact_Hosting 6 dias atrás	charlie 6 dias atrás	0	Qui Ago 23 17:16:07 2012
26821	Desfiguração de Site [.110.101]	pendente 8 dias atrás	Site_Abuse 7 dias atrás	charlie 2 dias atrás	0	Seg Ago 27 12:36:45 2012
26798	Desfiguração de Site [156.171]	pendente 8 dias atrás	Site_Abuse 8 dias atrás	charlie 8 dias atrás	0	Ter Ago 21 19:55:34 2012

60 tickets mais recentes sem proprietário

Novos e Abertos - Analistas

#	Assunto	Estado	Fila	Proprietário	Prioridade	Criado
26962	Malware Redirect [escenics.com]69.36.179.155]	aberto	Malware_Redirect	echo	0	2 dias atrás
26988	Erro de Código [www.241.32]	aberto	Site_Abuse	fox	0	2 dias atrás
27086	Hospedagem de software malicioso [200-98-68-236.clouduo1.com.br]200.98.68.236]	aberto	Malware_Hosting	golf	0	45 min atrás
27073	(Sem assunto)	novo	Malware_Redirect	golf	0	6 horas atrás



Tratamento de Incidentes – CTIR Gov



Filas no RT

Administração de filas

rt.ctir.gov.br/Admin/Queues/index.html

Ferramentas

Configuração

Usuários

Grupos

Filas

Campos Personalizados

Global

Ferramentas

Preferências

Aprovação

Filas Ativas

Selecionar uma fila:

#	Nome	Descrição	Endereço	Prioridade	PadrãodeVencimento	
9	Administracao	Eventos, cursos, colóquios, administracao de pessoal	ctir@ctir.gov.br/-	0-0	0	Ativado
15	Alerts	Alertas, Boletins, Announcements e Vulnerabilidades	ctir@ctir.gov.br/-	0-0	0	Ativado
13	Analista	Caixa postal do 'analista'@ctir.gov.br na Luminol	ctir@ctir.gov.br/-	0-0	0	Ativado
11	Artifact_Hosting	Notificação de incidentes com hospedagem de artefato	ctir@ctir.gov.br/-	0-0	0	Ativado
19	Botnets	Participação em botnets	ctir@ctir.gov.br/-	0-0	0	Ativado
1	General	The default queue	ctir@ctir.gov.br/-	10-0	2	Ativado
21	HoneyNet-Sensores	Sensores da HoneyNet.br e outros parceiros	-/-	0-0	0	Ativado
17	Leaks	Vazamento de informações (Pastes/Dumps/Exposures)	ctir@ctir.gov.br/-	0-0	0	Ativado
8	Malware_Analise	Analises de artefatos maliciosos	ctir@ctir.gov.br/-	0-0	0	Ativado
7	Malware_Hosting	Notificação de hospedagem de Malware	ctir@ctir.gov.br/-	0-0	0	Ativado
10	Malware_Redirect	Notificação de incidentes com Redirecionamento de Malware	ctir@ctir.gov.br/-	0-0	0	Ativado
16	Non_Statistical	Tiquetes nao considerados nas estatisticas (follow-ups, dfl-cert, respostas automaticas, etc)	ctir@ctir.gov.br/-	0-0	0	Ativado
14	Phishing_Message	Mesagens de phishing tratadas	ctir@ctir.gov.br/-	0-0	0	Ativado
20	Phishing_Site	Sítios falsos de instituições governamentais	-/-	0-0	0	Ativado
18	Scans	Scans de ssh, open proxy e outras atividades maliciosas de rede	ctir@ctir.gov.br/-	0-0	0	Ativado
3	Site_Abuse	Comprometimento de sítios da APF	ctir@ctir.gov.br/-	0-0	0	Ativado
6	SMTP_Abuse	Tratamento de Phishing (Cabeçalho)	ctir@ctir.gov.br/-	0-0	0	Ativado
5	[Mar_Abr] Old_Malware	Tratamento de Incidentes envolvendo Malware	ctir@ctir.gov.br/-	0-0	0	Ativado



Tratamento de Incidentes – CTIR Gov



Trâmite no RT

#27029: Atividade Suspeita

192.168.206.4/Ticket/Display.html

Ter Ago 28 12:47:59 2012 **Mauricio Leite - Estado alterado de 'novo' para 'aberto'**

Ter Ago 28 11:35:12 2012 **triagem - Dado a delta**

Ter Ago 28 11:34:44 2012 **triagem - Tomado**

Ter Ago 28 11:25:12 2012 **The RT System itself - Comentários adicionados** [Responder](#) [Comentário](#) [Reencaminhar](#)

1 última(s) notificações para [200.144.17.34]:

Nº do Ticket - Data de Criação GMT - Status - Dono - Assunto
=====

26512 - 14/08/2012 12:03:45 - resolved - fox - Atividade Suspeita/Maliciosa [200.144.17.34]
=====

Cia Proc. de Dados do Estado de S Paulo - Prodesp
csirt@sp.gov.br, admininternet@sp.gov.br

Ter Ago 28 11:25:12 2012 **The RT System itself - Assunto alterado de 'HoneyNet - Atividade Suspeita [200.144.17.34] - Pai:27026' para 'Atividade Suspeita/Maliciosa [200.144.17.34]'**

Ter Ago 28 11:25:12 2012 **The RT System itself - Filiação em ticket #27026 adicionada**

Ter Ago 28 11:25:12 2012 **HoneyNet-Parser - Tiquete criado** [Responder](#) [Comentário](#) [Reencaminhar](#)

Assunto: HoneyNet - Atividade Suspeita [200.144.17.34] - Pai:27026
Para: CTIR Gov <ctir@ctir.gov.br>
Date: Tue Aug 28 11:15:49 2012
From: HoneyNet-Parser <honeynet-parser@ctir.gov.br>

Aug 20 14:33:59.368088 200.144.17.34.1850 > xxx.xxx.xxx.25.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 767804308:767804308(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
Aug 20 14:33:59.838211 200.144.17.34.1850 > xxx.xxx.xxx.25.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 767804308:767804308(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
Aug 20 14:34:00.605038 200.144.17.34.1850 > xxx.xxx.xxx.25.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 767804308:767804308(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
Aug 27 16:04:10.650098 200.144.17.34.3464 > xxx.xxx.xxx.3.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 2227627216:2227627216(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
Aug 27 16:04:11.191725 200.144.17.34.3464 > xxx.xxx.xxx.3.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 2227627216:2227627216(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
Aug 27 16:04:11.626005 200.144.17.34.3464 > xxx.xxx.xxx.3.445: S (src OS: Windows XP SP1, Windows 2000 SP4) 2227627216:2227627216(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)

Baixar (sem título) / com cabeçalhos text/plain 458b

Baixar (sem título) / com cabeçalhos text/plain 1k



Tratamento de Incidentes – CTIR Gov



Template no RT

#27029: Atividade Suspeita

192.168.206.4/Ticket/Display.html

Ter Ago 28 12:48:00 2012 The RT System itself - cc admininternet@sp.gov.br adicionado

Ter Ago 28 12:47:59 2012 The RT System itself - Requestor abuse@sp.gov.br adicionado

Ter Ago 28 12:47:59 2012 The RT System itself - Requestor csirt@sp.gov.br adicionado

Ter Ago 28 12:47:59 2012 The RT System itself - Comentários adicionados

Responder Comentário Reencaminhar

Baixar (sem título) / com cabeçalhos
text/plain 3.9k

Prezados Senhores,

1. Informamos que o endereço IP [200.144.17.34] foi detectado por sensores apresentando possível atividade suspeita/maliciosa, conforme pode ser observado no log ao final desta mensagem.
2. A detecção foi realizada por meio de honeynet de um dos nossos colaboradores. O log fornecido é a única informação que nos foi provida e está em horário GMT.
 - 2.1. Verificamos que o IP em questão tentou acessar a porta 445 de mais de um dos nossos sensores (finais 3, 25), o que caracteriza varredura. Essa porta normalmente é utilizada para disponibilizar o serviço SMB (Server Message Block) usado para, entre outras coisas, compartilhar arquivos no Windows NT/2K/XP. Malwares podem ter originado essa atividade, por apresentarem comportamento semelhante ao registrado no log. Mais informações sobre essa porta podem ser encontradas em <http://www.speedguide.net/port.php?port=445>.
 - 2.2. Caso o endereço IP informado seja o de saída de sua rede e esteja utilizando NAT, sugerimos verificar os endereços comprometidos dentro de sua rede interna.
3. Qualquer tráfego para esses sensores pode ser considerado uma atividade suspeita, visto que a detecção foi realizada a partir de uma honeynet que não oferece nenhum serviço nem divulga sua existência. Portanto, o tráfego para essa honeynet caracteriza uma possível atividade maliciosa, proveniente de malwares ou de invasores, ou ainda acesso não intencional causado por falha nas configurações de equipamentos e softwares.
 - 3.1. Caso a investigação confirme a atividade suspeita/maliciosa, solicitamos que sejam tomadas as providências julgadas cabíveis para solucionar ou mitigar o incidente e que nos mantenham informados sobre as ações realizadas para a desinfecção ou contenção da atividade suspeita/maliciosa.
4. Esta mensagem foi copiada aos contatos abuse/técnico/administrativo. Caso esse tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
5. Qualquer referência futura a esta mensagem deverá conter o código indicado no campo "Assunto" desta mensagem.

Mais uma vez, colocamo-nos à disposição para auxiliá-los no que for necessário.

--
Atenciosamente,



Tratamento de Incidentes – CTIR Gov



Codificação de Scripts no RT

Modificar um scrip para a fila: X

192.168.206.4/Admin/Queues/Scrip.html?id=70&Queue=21

Ferramentas

Configuração

- Usuários
- Grupos

Filas

- HoneyNet-Sensores**
- Básicos
- Observadores

Scripts

- Modelos
- Campos Personalizados do Tiquete
- Campos Personalizados da Transação
- Direitos de Acesso do Grupo
- Direitos de Acesso de Usuário
- Histórico
- Campos Personalizados
- Global
- Ferramentas
- Preferências
- Aprovação

Campos de Scrip

Descrição: Na abertura, seta contatos e insere template

Condição: Definido pelo Usuário

Ação: Definido pelo Usuário

Modelo: AtividadeSuspeitaIP

Estágio: TransactionCreate

Apagar

Salvar as Alterações

Condições e ações definidas pelo usuário

(Use estes campos quando você escolher 'Definido pelo Usuário' para uma condição ou ação)

Condição personalizada:

```
##### Condição aplicável à ação descrita no Scrip #####
#
# Verifica 1 situação:
#
# 1. Se o status é alterado para "Open", satisfaz a condição, #
# contanto que o estado anterior seja "New"
#####
###-----
## Não satisfaz A NÃO SER que seja mudança de Status
return 0 unless $self->TransactionObj->Type eq "Status";
###-----
## Não satisfaz A NÃO SER que o novo estado seja "Aberto"
return 0 unless $self->TransactionObj->NewValue eq "open";
###-----
## Não satisfaz SE o estado anterior for "Novo"
return 0 unless $self->TransactionObj->OldValue eq "new";
###-----
# Declaração das Bibliotecas
use CtirGov::funcoesApoio;          # pacote do CTIR Gov
use DBI;                          # Acesso ao banco de dados.
```



Referências do RT

✓ Best Practical

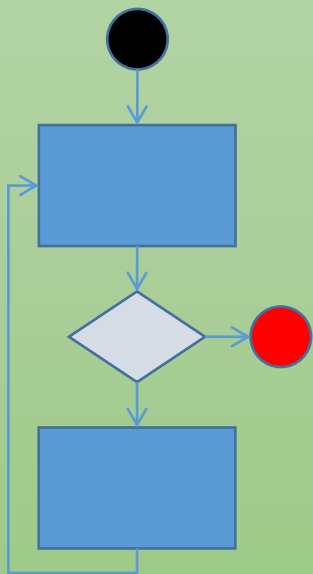
<http://www.bestpractical.com/rt/>

✓ RT Wiki

<http://www.requesttracker.wikia.com/wiki/HomePage>

Tipos de Incidentes

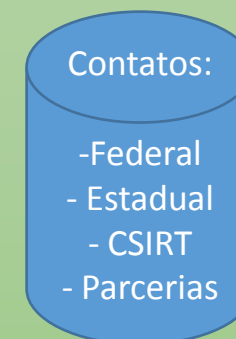
Processo/Metodologia



Modelos/Templates



Bases de Conhecimento





Tipos de Incidentes

- **Desfiguração de Sítio (*Defacement*)**
- **Abuso de Fórum/Comentários/Blogs**
- ***Spamdexing***
- ***Phishing Site***
- **Redirecionamento de Página**
- **Possível Vulnerabilidade**
- **Vazamento/Exposição de Dados Sensíveis (*Leaks*)**
- **Exposição de Código**
- ***Phishing Message/SMTP Abuse***
- ***Artifact and Malware Redirect/Hosting***
- **Varredura/Interceptação/Força Bruta (*Scan/Sniffing/Brute Force*)**
- **Negação de Serviço/Indisponibilidade (DoS/DDoS)**
- **Análise de Malware**



Tipos de Incidentes – Desfiguração de Sítio

Desfiguração de página (*Defacement*)

Desfiguração de página, *defacement* ou *pichação*, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

As principais formas que um atacante, neste caso também chamado de *defacer*, pode utilizar para desfigurar uma página *Web* são:

- explorar **erros da aplicação *Web***;
- explorar **vulnerabilidades do servidor de aplicação *Web***;
- explorar **vulnerabilidades da linguagem de programação** ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
- invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
- **furtar senhas de acesso à interface *Web* usada para administração remota.**

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do *site*, porém páginas internas também podem ser alteradas.

Tipos de Incidentes – Desfiguração de Sítio



HaCked by kinG oF coNTroL

Controlh4ck@Gmail.Com

AttCker From Saudi Arabia Hckers

[[Behind every success There is enemies]]

nux XXXXXXXXXXXXXXXXXXXX 2.6.18-374.18.1.el5.lve0.8.57 #1 SMP Fri Mar 3 _ 2012 x86_64
greetTs Todm3D | Game Over | AdooolE Tt3B | ÖŇÇİ ÇääİÊÊ | Cyber-Crystal | DrTaiGaR | XiOoOLX | DrBoOom



HACKED BY BRWSK007

KURDISH HACKERZ

hewa77w@yahoo.com



HaveE been haCked by kinG oF coNTroL

y8p@hoTmail.com

AttCker From Saudi Arabia Hckers

[[Behind every success There is enemies]]

Hacked by Havittaja & D4RKCR1PT3R

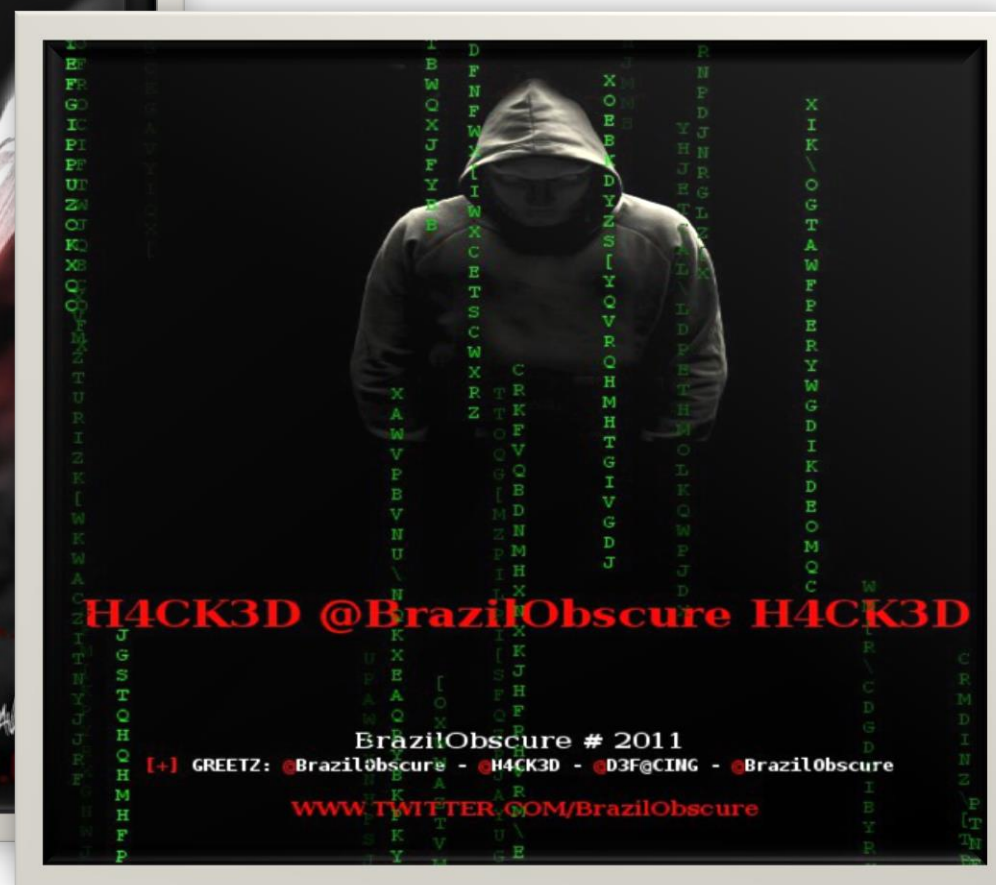




Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Desfiguração de Sítio





Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Desfiguração de Sítio - Notificação

Prezados Senhores,

1. Informamos a desfiguração do sítio, conforme anexo, em:

<http://xxx.gov.br/>

2. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à situação anterior ou a exclusão da(s) página(s) comprometida(s) pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasores para outras finalidades.

3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.

4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

--

Atenciosamente,

Equipe CTIR ctir@ctir.gov.br

www.ctir.gov.br

INOC-DBA (VOIP): 10954*810

#####

O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, da Casa Militar da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).

#####

CTIR Gov [999999]



Tipos de Incidentes – Desfiguração de Sítio - Spamdexing

Spam de links ou de conteúdos (*Spamdexing*)

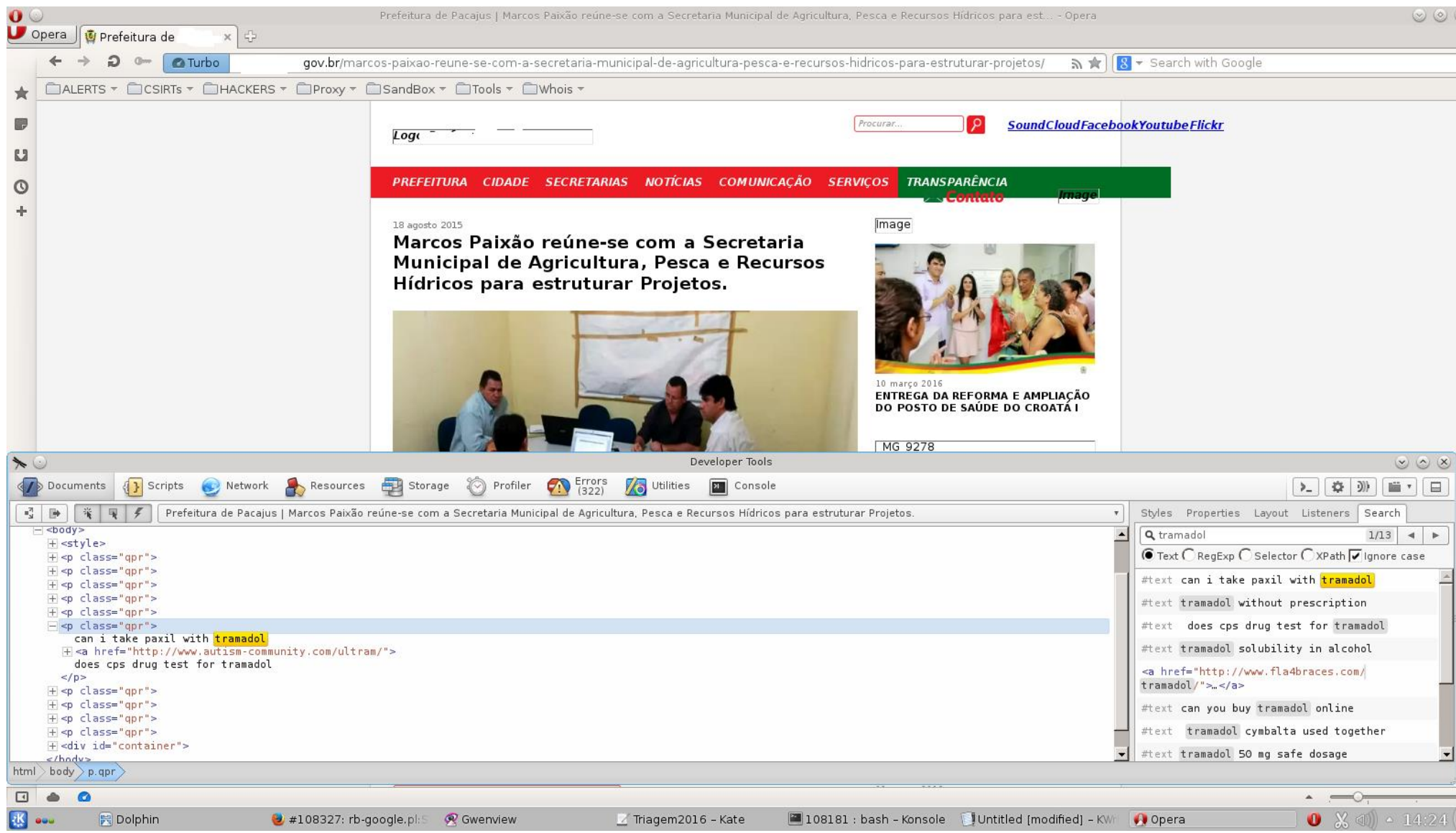
Também conhecido como **Spam de Busca**, **Spam de motores de busca**, **Web Spam** ou **Envenenamento de motores de Busca**, é a técnica de manipulação deliberada e maliciosa de mecanismos de buscas com o objetivo de **aumentar a relevância de um site em resultados de buscas**, ou seja, aumentar a chance de um site ser colocado no topo das páginas de resultados nos motores de busca.

É a prática de fazer modificações no código fonte de forma a enganar o **robot** e dar maior visibilidade a uma determinada página, colocando-a em melhores posições na página de resultados, ou ainda para influenciar a categoria à qual a página foi designada.

É uma técnica similar ao [Google bomb](#), mas com a diferença de ter **objetivos estritamente comerciais**.



Tipos de Incidentes – Desfiguração de Sítio - Spamdexing



Tipos de Incidentes – Desfiguração de Sítio - Spamdexing

【楽天市場】レーザーポインター パワーポイント (パソコン・周辺機器) の通販 - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

gov.br/responsive/index.php?id=20160321-11-16362

Most Visited ALERTS CSIRTs HACKERS Proxy SandBox Tools Whois RT

楽天市場 パソコン・周辺機器

買い物かご 総合案内 ヘルプ ご意見窓口 楽天トップへ 出店のご案内

お知らせ myクーポン 閲覧履歴 お気に入り 購入履歴

パソコン・周辺機器 レーザーポインター パワーポイント 検索 ショップ 全商品一覧

パソコン・周辺機器 ノートPC プリンタ 周辺機器 オフィス用品 レビュー あす楽 海外販売 オークション 商品価格ナビ 出店のご案内

iPadアクセサリ タブレットPC ウルトラブック モバイルデータ通信 中古PC インク 買取

SPU スーパーポイントアッププログラム カード・アプリ・モバイルで毎日**7倍!**

検索条件

お得なサービス

☐ スーパーDEAL対象

☐ 楽天プレミアム対象

検索する

ジャンル

全体へ

▼ パソコン・周辺機器

プリンタ・インク (27)

パソコンパーツ (3)

ディスプレイ・モニター (30)

パソコン周辺機器 (46)

アクセサリ (5)

マウス・キーボード・入力機器 (6)

トップ > パソコン・周辺機器 > 「レーザーポインター パワーポイント」の検索結果

楽天市場トップへ パソコン・周辺機器ジャンルトップへ

楽天カード入会で**5,000円分**ポイントプレゼント

すべての商品を一覧で表示する 同じ商品をまとめて表示する

並び替え 標準 詳細 画像

1件~45件 (全 445件)

在庫の有無 すべて表示 在庫あり・注文可能 カード決済 すべて表示 決済可能

【あす楽対象】 ロジクール ワイヤレスプレゼンテーションマウス 【2.4GHz・USB】 レーザーポイン...

ビックカメラ楽天市場店

レビュー (6件)

4580 円

最安ショップを見る

翌日配送



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Desfiguração de Sítio - Spamdexing

Prezados Senhores,

1. Informamos a desfiguração do sítio, com "spam de links/conteúdos", conforme anexo, em :

<http://xxx.gov.br/>

2. Detectamos que o incidente está relacionado ao ataque do tipo Spamdexing, que é a técnica de injetar, de forma deliberada e maliciosa, spams de links e de conteúdos em sítios. O objetivo do invasor é aumentar a relevância de sítios maliciosos ou de fins comerciais em motores de buscas e dessa forma melhor ranqueá-los nas consultas ao Google, Bing, Yahoo Search e outros.

2.1. Técnicas de dissimulação do ataque dificultam a sua percepção por parte do usuário. Pode-se verificar a invasão por meio dos passos:

(a) acessar a URL indicada;

(b) selecionar a opção "Exibir Código Fonte" do navegador; e

(c) procurar pelos termos: CHEAP – LEVITRA

2.2. Saiba mais sobre o Spamdexing (textos em inglês) em:

<http://www.webspam.org/seo-spam-what-is-spamdexing>

<http://en.wikipedia.org/wiki/Spamdexing>

2.3. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à situação anterior ou a exclusão da(s) página(s) comprometida(s) pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasores para outras finalidades.

3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.

4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

--

Atenciosamente,

Equipe CTIR ctir@ctir.gov.br

www.ctir.gov.br

INOC-DBA (VOIP): 10954*810

#####

O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, da Casa Militar da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).

#####

CTIR Gov [99999]



Tipos de Incidentes – Phishing Site

Página Falsa (Fake Website)

Normalmente, páginas falsas são **divulgadas a partir de mensagens fraudulentas**, que visam capturar dados pessoais ou institucionais (usuário/senha).

Podem ser **formulários sem quaisquer denominações** de empresa ou serviço, como também a **falsificação de portais válidos**.

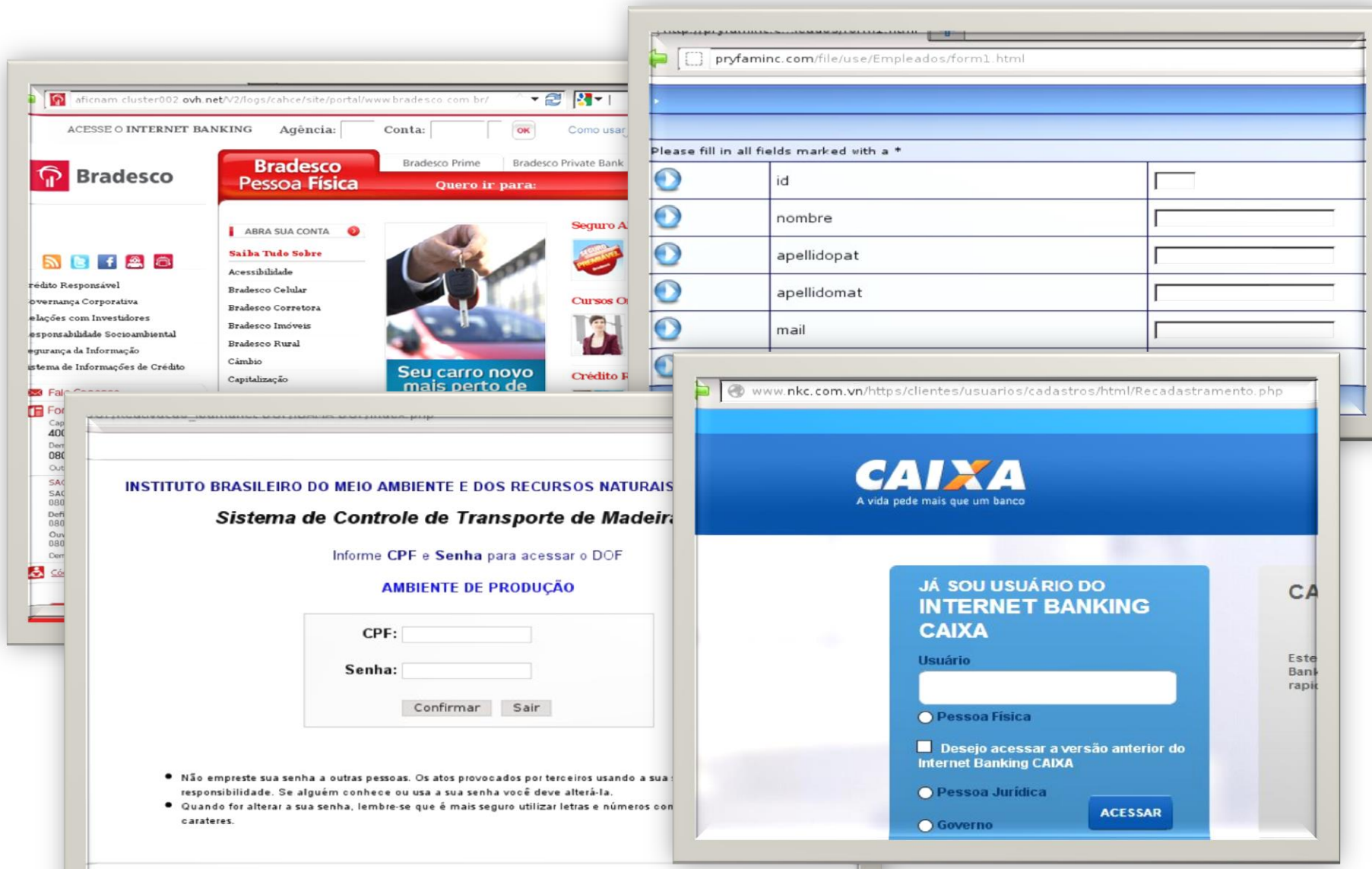
Por vezes, sites de governo são invadidos e acabam hospedando **páginas fraudulentas de instituições financeiras** (por exemplo).



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Site





Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Site

Prezados Senhores,

1. Verificamos a existência de página fraudulenta em:

<http://xxx.gov.br/> ou <http://xxx.com.br/www-gov-br/>

1.1 Sugerimos que o acesso ao site seja imediatamente bloqueado ou retirado da Internet.

2. Solicitamos que o incidente seja investigado e que nos mantenham informados sobre as ações realizadas.

3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.

4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

--

Atenciosamente,

Equipe CTIR ctir@ctir.gov.br

www.ctir.gov.br

INOC-DBA (VOIP): 10954*810

#####

O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, da Casa Militar da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).

#####

CTIR Gov [99999]



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Message

Falsificação de *e-mail* (*E-mail spoofing*)

Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que **consiste em alterar campos do cabeçalho de um *e-mail***, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Esta técnica é possível devido a características do protocolo SMTP (***S*imple *M*ail *T*ransfer *P*rotocol**) que permitem que campos do cabeçalho, como "From:" (endereço de quem enviou a mensagem), "Reply-To" (endereço de resposta da mensagem) e "Return-Path" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em **golpes de *phishing* (*phishing message* / *phishing-scam*)**. Atacantes utilizam-se de endereços de ***e-mail* coletados de computadores infectados para enviar mensagens** e tentar fazer com que os seus **destinatários acreditem que elas partiram de pessoas conhecidas**.



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Message

MENSAGEM ORIGINAL

De: xxx@xxx.gov.br<mailto:xxx@xxx.gov.br> [mailto:xxx@xxx.gov.br]

Enviada em: terça-feira, 6 de maio de 2014 02:25

Para: xxx

Assunto: Essas é as fotos atualizadas.

ANEXO: fotos_atualizadas.zip<<http://asp.trunojoyo.ac.id/wp-content/fotos.php>>

Ajude a reduzir o consumo de papel. Antes de imprimir, pense no seu compromisso com o MEIO AMBIENTE! Mas, se for imprimir, use a EcoFont (www.XXX.gov.br/ecofont<<http://www.XXX.gov.br/ecofont>>)

Ajude a reduzir o consumo de papel. Antes de imprimir, pense no seu compromisso com o MEIO AMBIENTE! Mas, se for imprimir, use a EcoFont (www.XXX.gov.br/ecofont)!



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Message

CABEÇALHO COMPLETO

Received: **from** xxx.gov.BR (x.x.112.107) **by** xxx.gov.BR
(x.x.113.39) with Microsoft SMTP Server (TLS) id 14.3.123.3; Tue, 6 May
2014 02:29:09 -0300

Received: **from** pps.filterd (smtp [127.0.0.1]) **by** smtp.xxx.gov.br
(8.14.5/8.14.5) with SMTP id s465QWvG029905 for <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
Tue, 6 May 2014 02:26:32 -0300

Received: **from** rdns-3.topserver3.com (**rdns-3.topserver3.com [189.1.164.113]**)
by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
Tue, 06 May 2014 02:26:32 -0300

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=default; d=topserver3.com;
h=From:Subject:To:Content-Type:MIME-Version:Date:Message-Id; i=abuse@topserver3.com<mailto:i=abuse@topserver3.com>;
bh=KrpV8sBt+XVpmUBp6/bgtUBnp3E=;
b=R6seHP/RgNeW7921LuHS0HuWaOhL2V3GUDWN9xWbdmJn+L+f+WFHHJOVT6pGwPG93ED2gir79Sgy
LizNDijolWNoHc6kmk3qGM7E536iu+X01uvSzs5B6WaSq7aBYI5RCZ3u87p6TUDUbdIWM5zHjIVm
XWLxdv7Pd7hbswwbu4g=

From: "xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>" <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>
Subject: =?iso-8859-1?Q?Essas_=E9_as_fotos_atualizadas.?=
To: <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>

Content-Type: multipart/alternative;
boundary="RIva3OkRT=_3xdJsGvFMRGCqfhHQZ1Jp5b"

MIME-Version: 1.0

Date: Tue, 6 May 2014 02:25:28 -0300

Message-ID: <20140506022527A0609EEE43\$E13001BB07@RIQUEZANC>



Tratamento de Incidentes – CTIR Gov



Tipos de Incidentes – Phishing Message

MALWARE REDIRECT

```
wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
--2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
Connecting ... connected.
Proxy request sent, awaiting response... 302 Moved Temporarily
Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar [following]
--2014-05-05 17:43:54-- http://www.nehirkoyekmegi.com/images/FOTO49029.rar
Connecting ... connected.
Proxy request sent, awaiting response... 200 OK
Length: 35939 (35K) [application/octet-stream]
Saving to: `FOTO49029.rar'
```

<http://www.virustotal.com/en/file/ee613ae08176fc1b6a4056d853bb3e5d4180d0e407be00dcfcbe4413bd3015c5/analysis/1399311981/>

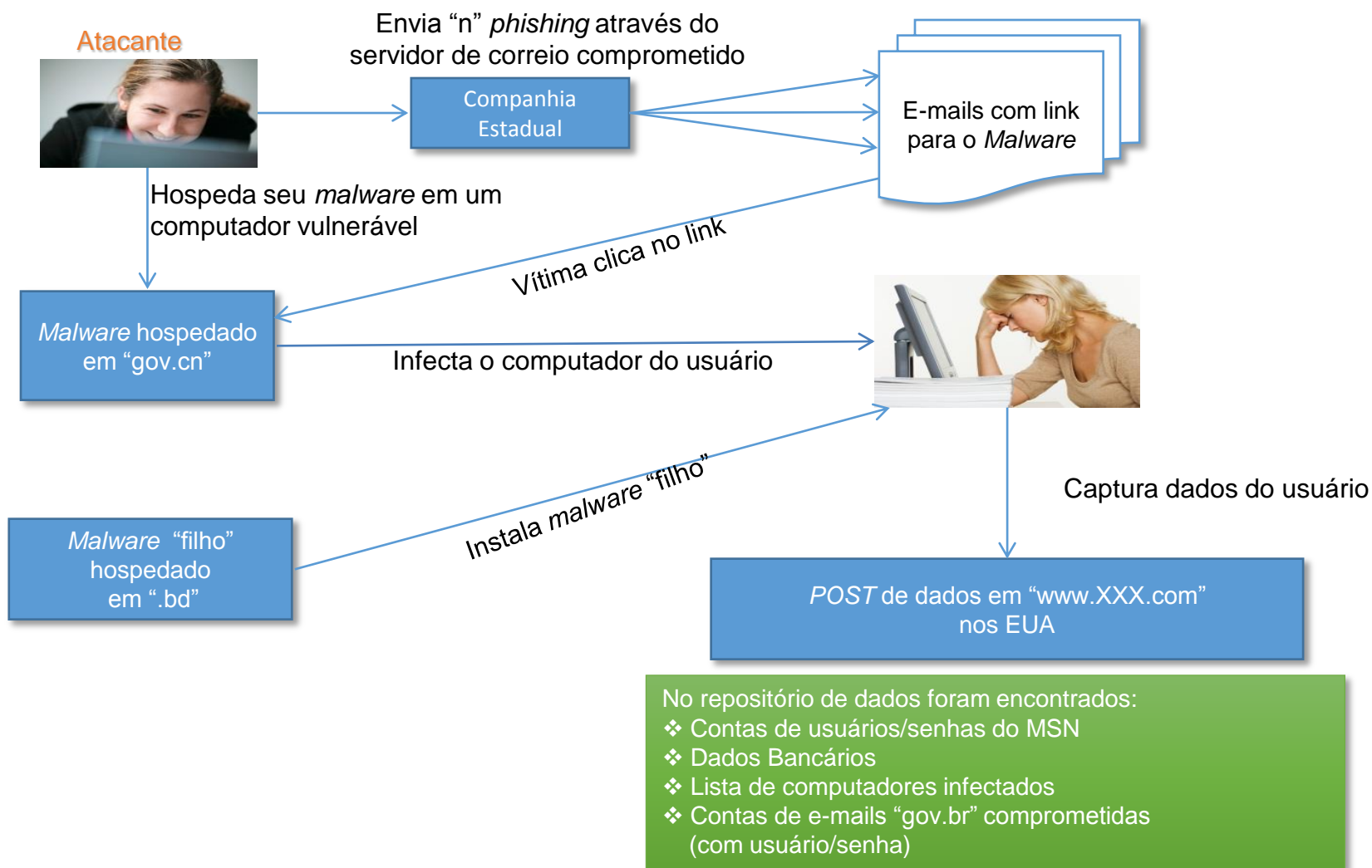
Detection ratio: **11 / 49**
Analysis date: **2014-05-05 17:46:21 UTC**

Detection ratio: **22 / 52**
Analysis date: **2014-05-10 06:26:59 UTC**

MALWARE HOSTING

```
wget http://www.nehirkoyekmegi.com/images/FOTO49029.rar
--2014-05-05 17:53:49-- http://www.nehirkoyekmegi.com/images/FOTO49029.rar
Connecting ... connected.
Proxy request sent, awaiting response... 200 OK
Length: 35939 (35K) [application/octet-stream]
Saving to: `FOTO49029.rar'
```

Engenharia Social (*phishing*) #15327





Engenharia Social (*phishing*) #15327

Tratamento do Incidente

1. Servidor de correio abusado (.gov) [BR]
2. Hospedagem do *malware* [CN]
-
3. Hospedagem do *malware* “filho” [BD]
4. Canal de controle do atacante [US]
-
5. E-mails comprometidos (gov.br) [BR]
6. Computadores infectados (gov.br) [BR]
7. Informações bancárias (Febraban) [BR]
8. E-mail comprometidos (MSN) [US]



Considerações Finais – CTIR Gov



Elementos de um código de conduta

CERT Coordination Center – CERT CC

1. Concentre-se nos pontos fortes do CSIRT.
2. Adapte-se à sua audiência.
3. Fale por você mesmo.
4. Não fale pelos outros.
5. Faça declarações completas.
6. Faça declarações concisas.
7. Evite o uso de jargões.
8. Use tato e diplomacia.
9. Evite ser arrogante.
10. Evite ser excessivamente informal.
11. Apresente fatos.
12. Seja sincero.
13. Mantenha controle.
14. Evite táticas agressivas.
15. Mantenha confidencialidade
16. Não faça promessas.
17. Ensine.
18. Enfatize o lado positivo.
19. Aplique controle de qualidade.
20. Use críticas construtivas.



Considerações Finais – CTIR Gov



Rest1.pdf Banco do Brasil CERT.br: Documentos Disp

www.cert.br/docs/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

15 ANOS

Sobre o CERT.br
CSIRTs
Estatísticas
Cursos
Projetos
Publicações
Palestras
Links
FAQ
Mapa do site
Contato
Twitter
RSS

Busca
ok
Buscar em CERT.br

W3C XHTML 1.0 W3C CSS
Acessibilidade do site

Núcleo de Informação e Coordenação do Ponto BR

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTR.O.br - W3C.br

Você está em: CERT.br > Publicações

English
Imprensa

Documentos Disponíveis em Português

White Papers

[Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço \(DDoS\)](#) novo
Autor: CERT.br

[Recomendações para Notificações de Incidentes de Segurança](#) atualizado
Autor: CERT.br

[Resultados Preliminares do Projeto SpamPots: Uso de Honeypots de Baixa Interatividade na Obtenção de Métricas sobre o Abuso de Redes de Banda Larga para o Envio de Spam](#)
Autor: CERT.br

[Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos](#)
Autores: Cristine Hoepers, Klaus Steding-Jessen, Nelson Murilo, Rafael R. Obelheiro

[Honeypots e Honeynets: Definições e Aplicações](#)
Autores: Cristine Hoepers, Klaus Steding-Jessen e Marcelo H. P. C. Chaves

[Sugestões para defesa contra ataques de força bruta para SSH](#)
Autor: Nelson Murilo

Documentos Produzidos pelo CERT.br

[Documentos e Palestras do CERT.br no Escopo do seu Trabalho na CT-Spam](#)

[Cartilha de Segurança para Internet](#)

[Práticas de Segurança para Administradores de Redes Internet](#)

[FAQ: Perguntas Frequentes ao CERT.br](#)

[FAQ: Dúvidas Frequentes ao Reportar Ataques](#)

Documentos Traduzidos pelo CERT.br

[CERT/CC CSIRT FAQ](#)

[Criando um Grupo de Respostas a Incidentes de Segurança em Computadores: Um Processo para Iniciar a Implantação](#)

[Advisories do CERT/CC \(Traduções descontinuadas\)](#)

Apresentações e Eventos



Obrigado !

Maurício Leite

ctir@ctir.gov.br
mauricio.leite@presidencia.gov.br

3411-2308