



# CTIR Gov



## *CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO*



## Colóquio Técnico de ETIRs 2017

*Maurício Leite Ferreira da Silva*  
*Analista de Incidentes*

TLP: BRANCO





# CTIR Gov

## Objetivos

O objetivo da apresentação é 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 a evolução do nível de maturidade adquirido pelo CTIR Gov, ao longo do tempo de sua criação até o presente momento e os desafios éticos para ETIRs.



# CTIR Gov



DOU Nº 143, quinta-feira, 27 de julho de 2017

**PRESIDÊNCIA DA REPÚBLICA  
GABINETE DE SEGURANÇA INSTITUCIONAL**

## Organograma

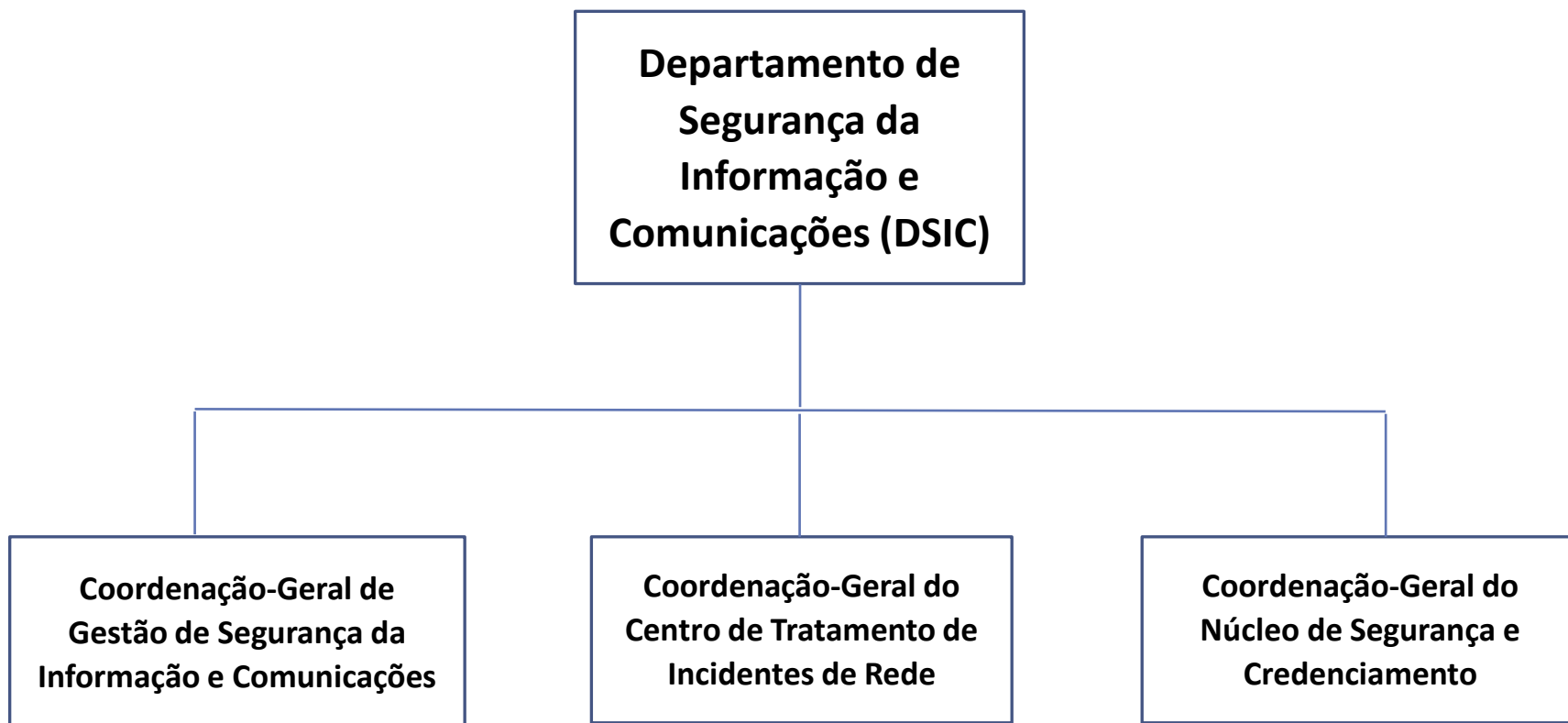




# CTIR Gov



DOU Nº 143, quinta-feira, 27 de julho de 2017





# CTIR Gov



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





# CTIR Gov



Instrução Normativa GSI/PR Nº 1 - 2008

*(Art. 2º - IN01/DSIC/GSIPR)*

Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade**, a **Autenticidade**.

**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.



# CTIR Gov



## 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;





# CTIR Gov



## 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.



# CTIR Gov



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.



# CTIR Gov



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.



# CTIR Gov



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.



# CTIR Gov



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.



# CTIR Gov

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***



# CTIR Gov



## NC 05/2009 – Criação de ETIRs

**BOLETIM DE PESSOAL E SERVIÇO**  
 MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

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

**Sumário**

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO ..... 3  
 SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO ..... 3

**SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO**

PORTARIAS SLTI DE 25 DE MARÇO DE 2011

Nº 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 de competência que lhe confere a Portaria nº 56, de 23 de fevereiro de 2011, o disposto no Decreto nº 3.505, de 13 de junho de 2000, no Decreto nº 4.553, de 27 de dezembro de 2002, na Norma Complementar nº 05, 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. 1º Instituir o Centro de Tratamento e Resposta a Ataques na Rede MP - CeBra, no âmbito do Ministério do Planejamento, Orçamento e Gestão, Departamento Setorial de Tecnologia da Informação da Secretaria de Logística e Tecnologia da Informação - DISTIS/SLTI, com as seguintes atribuições na Política de Segurança da Informação e Comunicações e pelo Gabinete de Segurança Institucional da Presidência da República - CIGSI:

Art. 2º O Centro de Tratamento e Resposta a Ataques na Rede MP - CeBra será a Equipe de Tratamento em Incidentes de Redes Computacionais - ETIR do Ministério do Planejamento.

Art. 3º O CeBra tem por missão "Garantir a Segurança da Informação e Comunicações no âmbito do Ministério do Planejamento, por meio do estrito cumprimento da Política de Segurança, suas normas e da gestão de riscos controlada".

Art. 4º O CeBra 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, divulgar 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 e análise de 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 da organização;
- VII - Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes;
- VIII - Cooperar com outras equipes de Tratamento e Resposta a Incidentes computacionais; e
- IX - Participar em fóruns, redes nacionais e internacionais.

Art. 5º As proposições de que trata o art. 2º desta Portaria serão submetidas ao Comitê de Segurança da Informação e Comunicações - CSIC do Ministério.

Art. 6º A ETIR CeBra adotará o modelo de implementação combinado ou misto onde poderá atuar uma ETIR central (CeBra) e equipes descentralizadas no âmbito do Ministério do Planejamento, supervisionadas pela ETIR CeBra.

Art. 7º O agente responsável pela ETIR será designado por meio de Portaria própria.

Art. 8º A ETIR CeBra será composta por membros da Coordenação de Suporte Tecnológico, da Coordenação-Geral de Tecnologia da Informação, do Departamento Setorial de Tecnologia da Informação, da Secretaria de Logística e Tecnologia da Informação - COTECH/SLTI/SLTI.

Art. 9º As demais unidades administrativas do Ministério serão convidadas a indicar membros para compor a ETIR CeBra, desde que devidamente treinados e orientados e, comprovados os conhecimentos específicos na área de Segurança da Informação e Comunicações.

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

Parágrafo único. Para cada membro da ETIR CeBra deverá ser designado um substituto devidamente treinado e orientado para dar suporte e designado o ETIR.

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

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

Nº 14 -

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

O GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, no uso de competência que lhe confere a Portaria nº 56, de 23 de fevereiro de 2011, o disposto no Decreto nº 3.505, de 13 de junho de 2000, no Decreto nº 4.553, de 27 de dezembro de 2002, na Norma Complementar nº 05, 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. 1º Designar o Coordenador de Suporte Tecnológico do Departamento Setorial de Tecnologia da Informação da Secretaria de Logística e Tecnologia da Informação - COTECH/SLTI como Agente Responsável pelo Centro de Tratamento e Resposta a Ataques na Rede MP - CeBra no âmbito do Ministério do Planejamento, Orçamento e Gestão, com as seguintes atribuições na Política de Segurança da Informação e Comunicações e pelo Gabinete de Segurança Institucional da Presidência da República.

Art. 2º Atribuir ao Agente Responsável pelo Centro de Tratamento e Resposta a Ataques na Rede MP - CeBra as seguintes competências:

- I - Coordenar e acompanhar:
  - a) as atividades de tratamento e resposta a incidentes nas redes computacionais do Ministério;
  - b) a análise dos sistemas comprometidos buscando causas, danos e responsabilidades;
  - c) a avaliação, auditoria e testes das condições de segurança das redes computacionais do Ministério;
  - d) e análise dos ativos de informação e estruturas constitutivos dos ambientes de tecnologia da informação, presentes no Ministério;
- II - Coordenar, acompanhar e orientar as equipes no reparo a danos causados por incidentes de segurança;
- III - Executar outras atividades correlatas que lhe forem demandadas.
- IV - Participar, juntamente com o Gestor de Segurança da Informação e Comunicações, na proposição de recursos necessários às ações de segurança da informação e comunicações;
- V - Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes nas redes computacionais do Ministério;
- VI - Participar da definição e acompanhar os indicadores de acompanhamento de incidentes nas redes computacionais do Ministério;
- VII - Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos relacionados à segurança da informação e comunicações;
- VIII - Planejar, coordenar, supervisionar e orientar a execução das atividades da respectiva unidade;
- IX - Assessorar o CTIR GOV com as informações necessárias à atualização e manutenção das bases de dados de incidentes do Ministério;
- X - Assessorar a autoridade competente nos assuntos pertinentes à sua área de atuação; e
- XI - Desenvolver um Plano de Consolidação em segurança da informação e comunicações a fim de que todos os servidores do MP tenham ciência do assunto.

Art. 3º As proposições de que trata o art. 2º desta Portaria serão submetidas ao Comitê de Segurança da Informação e Comunicações - CSIC do Ministério para aprovação.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

FERNANDO ANTÔNIO BRAGA DE SIQUEIRA JÚNIOR

**SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO**

PORTARIAS SPOA DE 25 DE MARÇO DE 2011

Nº 115 - O SUBSECRETÁRIO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO, DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, no uso de competência que lhe foi delegada pela Portaria GM/MP nº 54, de 18 de junho de 2003, e nos termos de Lei nº 9.327, de 9 de dezembro de 1996, resolve:

Autorizar, em caráter excepcional e no prazo de 1 (um) ano, o servidor Jorge Macedo de Souza, lotado na Superintendência do Patrimônio da União no Estado de Rondônia, SIAPE nº 0707765, RG nº 124713 - SSP/RR, CNH nº 831638630, e Registro nº 02184065864, Categoria B, e conduzir veículo oficial de propriedade deste Ministério, para uso exclusivo em serviço e no seu horário de funcionamento, conforme estabelecido na Portaria MP/GO nº 140, de 8 de setembro de 1995.

Nº 117 - O SUBSECRETÁRIO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO, DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, no uso de competência que lhe foi delegada pela Portaria GM/MP nº 54, de 18 de junho de 2003, e nos termos de Lei nº 9.327, de 9 de dezembro de 1996, resolve:

Autorizar, em caráter excepcional e no prazo de 1 (um) ano, o servidor Flávio Aníbal Franco de Medeiros, lotado na Superintendência do Patrimônio da União no Estado de



# CTIR Gov



NC 05/2009 – Criação de ETIRs

## 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;





# CTIR Gov



## 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.



# CTIR Gov



## 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;



# 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

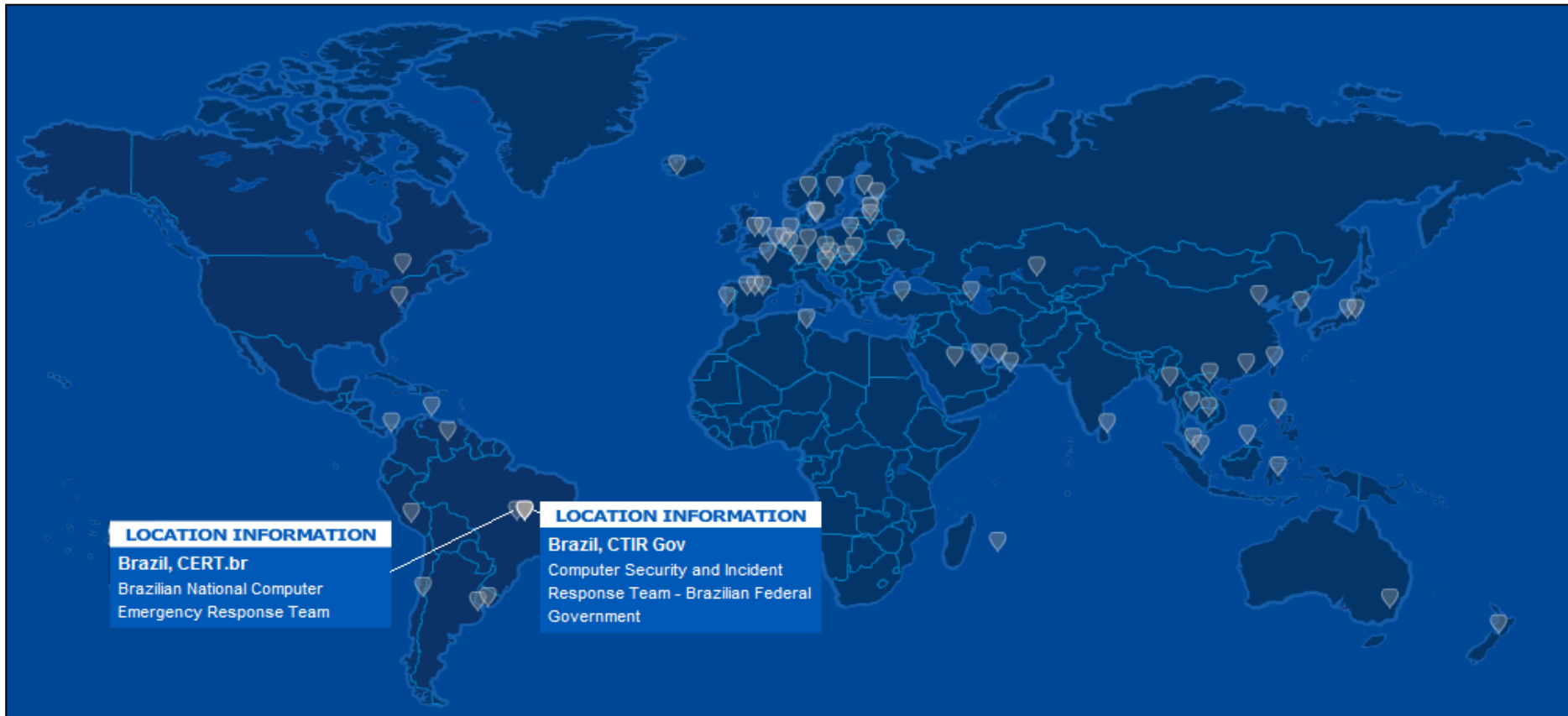
Composta por todos os órgãos e entidades da APF direta e indireta. Em caráter excepcional e de forma colaborativa os órgãos dos Estados e Municípios, pertencentes aos domínios “**gov.br**”, “**jus.br**”, “**leg.br**”, “**mil.br**”, “**mp.br**” e outros.



# CTIR Gov



## CSIRTs com responsabilidade nacional no mundo



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



# CTIR Gov



**2017**

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



# CTIR Gov



## Serviços Realizados

### Capacitação

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

### Integração com outros atores:

- 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;

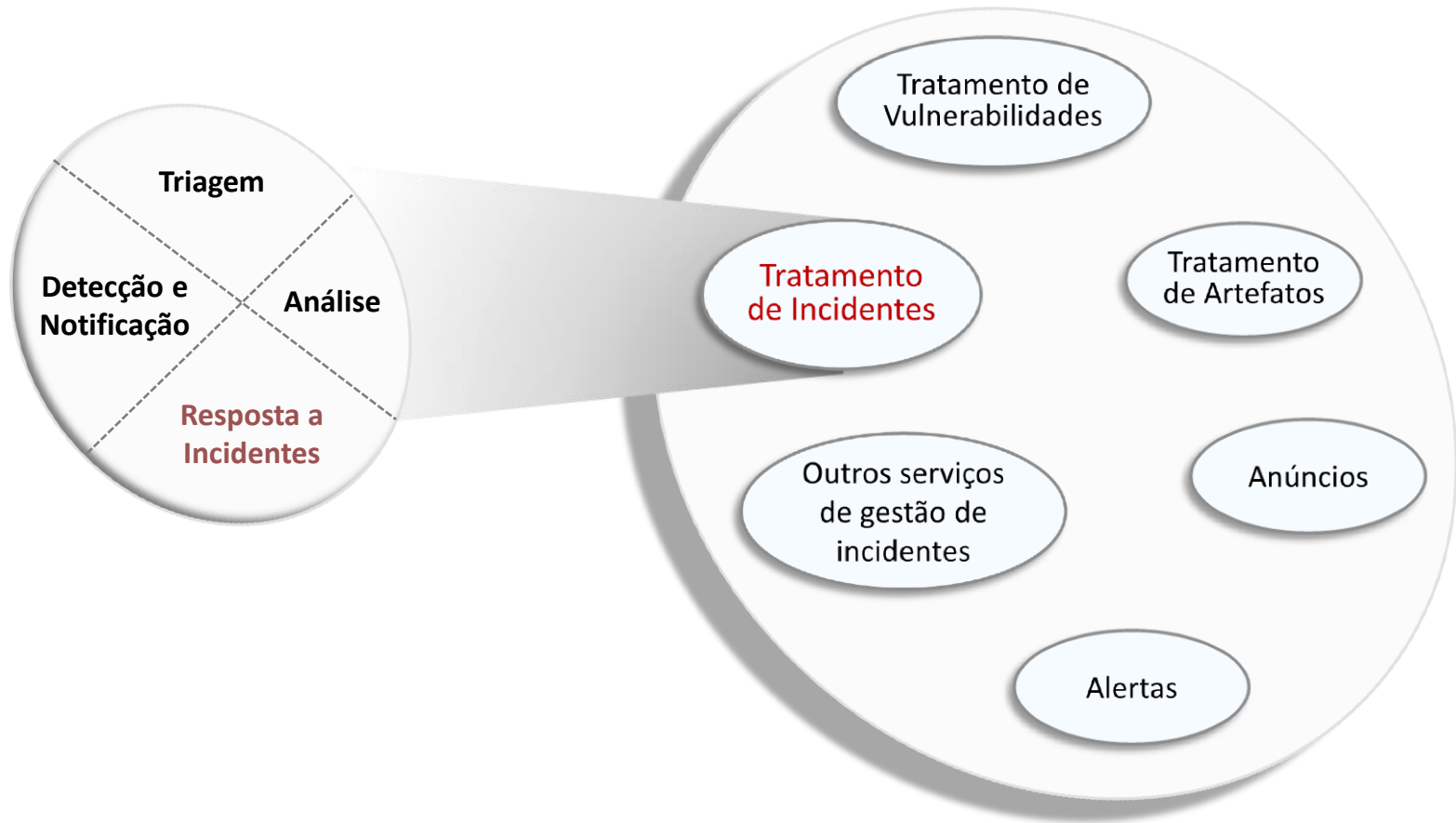
### Domínios

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



# CTIR Gov

## Gestão de Incidentes





# CTIR Gov

## Robôs

- Rb-Google
- Rb-Zone-h
- Rb-Twitter
- Rb-WebSiteTester





# CTIR Gov

## Robôs

### RB-GOOGLE

O Robô Google é um programa escrito em PERL e que usa bibliotecas com funções e objetos de cliente web para acessar as URL's utilizando os Mecanismos de Busca do Google Search - GSS, Google Search Engine – GSE, Google Developers - GDG e também realiza GET's para verificar o conteúdo de páginas oficiais.

<http://www.google.com.br/search?q=tags site:dominio.gov.br>

Verifica abuso de sítios que podem conter:

- Desfiguração
- Spamdexing
- Abuso de Fórum
- Exposição de Código
- Listagem de Diretórios
- Possíveis Vulnerabilidades



# CTIR Gov Robôs



## Comandos Google Search

RB-GOOGLE

allinanchor: - usa-se esta palavra para buscar a palavra pesquisada nos links das páginas.

inanchor: - as buscas trarão resultados nos quais os termos aparecerão em textos ancôras de links para as páginas.

allintext: - todos os termos pesquisados aparecerão nos textos das páginas localizadas.

intext: - termos que aparecem no texto da página.

allintitle: - as buscas reportarão resultados que apareçam nos títulos das páginas.

title: - dos resultados obtidos aparecerão somente os que aparecerem no título da página.

allinurl: - resultados trazem as palavras na URL da página.

inurl: - termos que aparecem na URL de determinado site.

date: - faz buscas entre intervalos de meses ;

site: - busca diretamente dentro de um domínio;

\$...\$ - busca termos entre determinados valores;

filetype: - busca arquivos de uma específica extensão;

link: - busca páginas que apontam para determinada URL;



# CTIR Gov Robôs



## Comandos Google Search

## RB-GOOGLE

safeSearch: - essa busca exclui conteúdo adulto (ex.: safeSearch: tecnologia mulheres);

autor: - busca publicações de um autor específico;

group: - busca mensagens de um grupo específico;

insubject: - busca mensagens que contenham determinada palavra ou termos no título;

location: - busca notícias cuja origem esteja em um determinado local ;

source: - faz buscas de notícias com determinada origem ;

book ou books - busca resultados que aparecem por completo o nome dos livros ;

define, what is, what are - busca por significados para determinada palavra ou expressão;

define: - procura por resultados com a definição de palavras ou frases na Internet;

phonebook: - faz buscas em listas telefônicas ;

bphonebook: faz buscas em listas telefônicas comerciais ;

rphonebook: faz busca em listas telefônicas residenciais ;

movie: - busca por resenhas e comentários de filmes;



# CTIR Gov Robôs



## Comandos Google Search

stocks: - faz buscas por informações sobre ações ;

weather - busca a previsão de tempo;

cache: - busca a última versão da URL indexada pelo Google ;

info: ou id: - procura informações sobre determinado domínio ;

related: - busca páginas relacionadas ou semelhantes à URL .

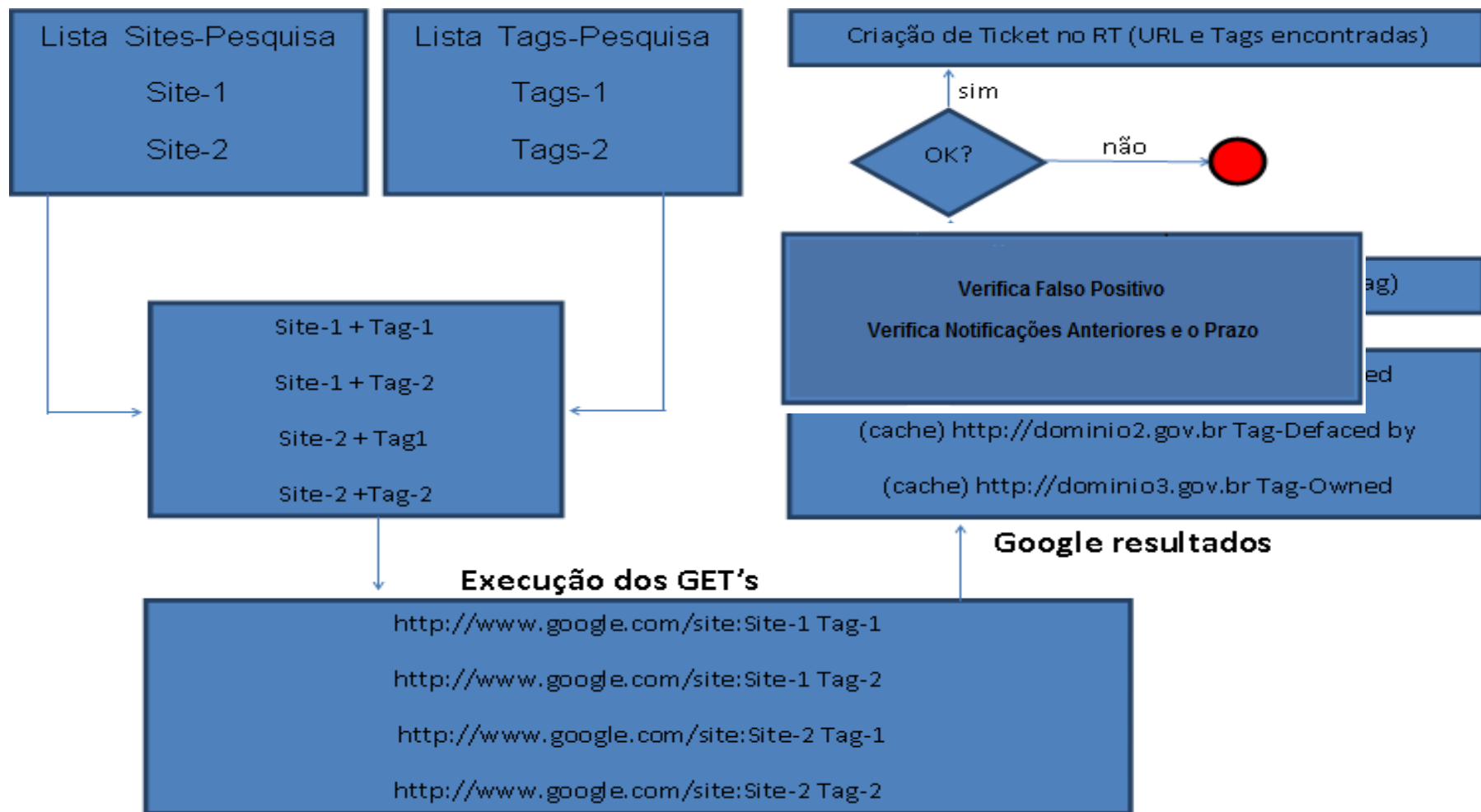
RB-GOOGLE



# CTIR Gov

## Robôs

RB-GOOGLE





# CTIR Gov Robôs



RB-GOOGLE



هلا بألى له الخافق يهلي

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.e15.lve0.8.57 #1 SMP Fri Mar 3 \_ 2012 x86\_64  
greeTs To:dm3D | Game Over | AdoOolE Tt3B | ÖÑçl ÇââîÈÈ | Cyber-CrystaL | Dr.TaiGaR | XlOoOLX | Dr.BoOom

Hacked by Havittaja & D4RKCR1PT3R



HACKED BY BRWSK007

KURDISH HACKERZ

hewa77w@yahoo.com



HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N!  
HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N!  
HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N! HWZ!EQ!S!C!N!

Have been haCked by kinG oF coNTroL

y8p@hoTmaiL.com

AttCker From Saudi Arabia Hckers

[[ Behind every success There is enemies ]]

id - Greet!id - Greet!groups - Greet!T!bin - Greet!owen - Greet!Azed - Greet!1Dreter



# CTIR Gov Robôs



RB-GOOGLE





# CTIR Gov

## Robôs



RB-GOOGLE

The screenshot shows a web browser window displaying a news article on the website gov.br. The article is dated 18 agosto 2015 and is titled "Marcos Paixão reúne-se com a Secretaria Municipal de Agricultura, Pesca e Recursos Hídricos para estruturar Projetos." Below the title is a photograph of a meeting. To the right of the article is a sidebar with a section titled "ENTREGA DA REFORMA E AMPLIAÇÃO DO POSTO DE SAÚDE DO CROATÁ I" dated 18 março 2016, accompanied by another photograph. The browser's address bar shows "gov.br/reune-se" and "ra-estruturar-projetos/". The search bar contains the text "tramadol". Below the browser window, the Developer Tools are open, showing the HTML structure of the page. The search results for "tramadol" are visible in the right-hand pane of the Developer Tools, listing various search results such as "can i take paxil with tramadol" and "tramadol without prescription".





# CTIR Gov Robôs



RB-GOOGLE

The screenshot shows the Rakuten website interface. At the top, there's a navigation bar with 'File Edit View History Bookmarks Tools Help' and a search bar containing '【楽天市場】レーザーポインター パ...'. The address bar shows 'gov.br/responsive/index.php?id=20160321-11-16362'. Below the navigation, there are several utility buttons like '買い物かご', 'お知らせ', 'myクーポン', '閲覧履歴', 'お気に入り', and '購入履歴'. The main content area features a search bar with 'レーザーポインター パワーポイント' and a search button. Below the search bar, there are category links like 'ノートPC', 'プリンタ', '周辺機器', and 'オフィス用品'. A large banner for 'スーパーポイントアッププログラム' (Super Point Up Program) is displayed, along with a promotion for '楽天カード入会で5,000円分ポイントプレゼント' (Rakuten Card membership with 5,000 yen worth of points gift). The search results section shows 'すべての商品を一覧で表示する' (Display all products) and '同じ商品をまとめて表示する' (Display similar products together). The product list includes '【あす楽対象】 ロジカル 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...' with a price of 4580円. The bottom of the page shows the system tray with various open applications like Dolphin, Gview, and Opera.



# CTIR Gov Robôs



RB-GOOGLE

Habitação — Prefeitura Municipal de Konqueror

File Edit View Go Bookmarks Tools Settings Window Help

http://www... .gov.br/foruns/habitacao

Acessar

Mapa do Site Acessibilidade Contato

Buscar no Site Buscar

Página Inicial | Fóruns | Ouvidoria | Perguntas Frequentes | RSS

Você está aqui: Página Inicial / Fóruns / Habitação

**Sobre o Município**

- História do Município
- Como Chegar
- Notícias
- Agenda de Eventos
- Galeria de Fotos
- Galeria de Vídeos

**Administração**

- Gabinete do Prefeito

## Habitação

por Interlegis — última modificação 01/03/2017 12h28

Um nível acima

Debates sobre moradia e habitação em nosso município.

Exibir somente tópicos não-respondidos

Iniciar um novo tópico

Tópico	Respostas	Comentários recentes
 por administrador	Nenhuma resposta ainda.	por administrador Sábado 11:00
Hackeado por m1n3r4d0r por admin	Nenhuma resposta ainda.	por admin Quinta 21:59

Find: hacke Next Previous Options

Portal da Transparência

Acesso a Informação

e-SIC Ouvidoria

Webmail

Protocolo

Mídias Sociais



# CTIR Gov Robôs



RB-GOOGLE

A captura de tela mostra uma janela de navegador com o endereço `http://www.____.gov.br/legislacao/tipo/`. O cabeçalho da página contém o texto "Prefeitura Municipal de" e "Administrando para todos". Um menu de navegação azul na base da página inclui links para "A PREFEITURA", "SECRETARIAS", "PUBLICAÇÕES", "LEGISLAÇÃO" e "TRANSPARÊNCIA FISCAL".

Na parte inferior da página, uma mensagem de erro em vermelho indica: **Fatal error:** Call to a member function `getNome()` on a non-object in `/home/...../public_html/view/pages/legislacoes/detalhar.php` on line **30**.



# CTIR Gov Robôs



RB-GOOGLE



## Index of /suporte/includes

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">classes/</a>	05-May-2015 13:10	-	
<a href="#">common/</a>	09-Aug-2012 08:45	-	
<a href="#">config.inc.php</a>	21-Aug-2015 09:26	3.5K	
<a href="#">config.inc.php-dist</a>	21-Aug-2015 09:26	3.5K	
<a href="#">css/</a>	09-Aug-2012 08:45	-	
<a href="#">fckeditor/</a>	09-Aug-2012 08:45	-	
<a href="#">functions/</a>	09-Aug-2012 08:45	-	
<a href="#">help/</a>	09-Aug-2012 08:45	-	
<a href="#">icons/</a>	09-Aug-2012 08:45	-	
<a href="#">imgs/</a>	09-Aug-2012 08:45	-	
<a href="#">include_geral.inc.php</a>	21-Aug-2015 09:26	1.5K	
<a href="#">include_geral_II.inc.php</a>	21-Aug-2015 09:26	54	
<a href="#">js/</a>	09-Aug-2012 08:45	-	



# CTIR Gov

## Robôs



RB-GOOGLE

sex, 7 de jul de 2017 10:03:24 Robo-Google - Tíquete criado  
Assunto: rb-gss.pl - [xxx.xx.gov.br | 200.xxx.xxx.xxx]  
Para: CTIR Gov <ctir@ctir.gov.br>  
Date: Fri Jul 7 09:03:23 2017  
From: Robo-Google [rb-google@ctir.gov.br](mailto:rb-google@ctir.gov.br)

Dominio:xxx.xx.gov.br  
IP:200.xxx.xxx.xxx  
Nr\_URLs:1

1.  
URL:<https://xxx.xx.gov.br/commit/1006bc11f964b341>  
Motivo:Desfiguracao  
Tags encontradas:Hacked by  
Nr ocorrencias tags:3x no HTML da URL.



# CTIR Gov Robôs



RB-ZONE-H



[Home](#) [News](#) [Events](#) [Archive](#) [Archive](#) [Onhold](#) [Notify](#) [Stats](#) [Register](#) [Login](#)

**Mirror saved on:** 2017-07-26 16:50:31

**Notified by:** TeaM\_CC

**Domain:** <http://districtcourtsbuner.gov.pk/skidie.txt>

**IP address:** 192.169.80.198

**System:** Linux

**Web server:** LiteSpeed

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-07-26 16:50:31

```
hacked by skidie khan  
#TeaM_CC
```



# CTIR Gov

## Robôs



RB-ZONE-H

qua, 26 de jul de 2017 16:10:22 Robo-Zone-H - Tíquete criado

Assunto: rb-zone-h.pl - [www.xxx.xx.gov.br|198.xxx.xxx.xxx]

Para: CTIR Gov <ctir@ctir.gov.br>

Date: Wed Jul 26 15:10:21 2017

From: Robo-Zone-H [rb-zone-h@ctir.gov.br](mailto:rb-zone-h@ctir.gov.br)

Dominio:www.xxx.xx.gov.br

IP:198.xxx.xxx.xxx

Nr\_URLs:1

1.URL:http://www.xxx.xx.gov.br/noticias.php

Motivo:Desfiguracao Zone-h

Tags encontradas:yOSHI Team

Link Descricao:www.zone-h.org/mirror/id/24137186

Snapshot:zonehmirrors.net/defaced/2015/04/26/www.xxx.xx.gov.br/noticias.php/w  
ww.xxxx.xx.gov.br/noticias.php

Data Snapshot:26/04/2015 02:39:27

Data Triagem:26/07/2017



# CTIR Gov

## H4CK M1RROR



MIRROR-H | Mirror | Hack Zone | H@CK MIRROR ZONE | Special Att...

www.hack-mirror.com/special.html

# H4CK M1RROR

HOME ATTACKS ARCHIVE SPECIAL ATTACKS ONHOLD ATTACKS NOTIFY ATTACKS ATTACKERS RANKING TEAMS RANKING FACEBOOK

Home Special Attacks Server Time: 12:10:40 Search... All In Onhold

## Special Attacks

**Legends**

- H - Homepage defacement
- R - Redefacement (click to view all defacements of this site)
- ★ - Special defacement (special defacements are important websites)
- M - Mass defacement (click to view all defacements of this IP)
- L - Location of Server according to IP address

Total deface: **23747** Home Deface: **10358** Special Deface: **23747** Unique IP: **7557**

Time (UTC)	Attacker	Team	H	M	R	L	★	Domain	OS	View
2017-11-21 06:18:48	TRIPLE R	BANGLADESH CYBER GHOST	H				★	shopasia.co.in	Linux	Mirror
2017-11-21 05:09:58	World Potent Devil	BANGLADESH CYBER GHOST	H				★	www.mastermindtravels.in	Linux	Mirror
2017-11-21 00:26:29	X-m3n	X-protocol					★	.....gov.br/X-m3n.html	Linux	Mirror
2017-11-21 00:07:05	X-m3n	X-protocol					★	.....gov.br/X-m3n.html	Linux	Mirror

10:10 22/11/2017





# CTIR Gov

## MIRROR H



MIRROR-H | Mirror | Hack Zone X H@CK MIRROR ZONE | Special Att. X +

http://intra.presidencia.gov.br

MIRROR-H.ORG ANA SAYFA Bildiri Yap MASS (çoklu) Korsan Arşivler Yasal Uyarı İletişim

562407 Zone Kaydı! 20876 Hacker! 3 Duyuru!

Detaya Git! Detaya Git! Detaya Git!

SON KAYITLAR

Hacker	Ülke	Scheme	Host	Path	Query	Tarih	izle
Turkhacks.com	USA	http	northpolefashion.com			22 Kasim 2017	Q
DarkBat	USA	http	northpolefashion.com	/		22 Kasim 2017	Q
MindPowerSec	BRA	http	██████████.com.br			22 Kasim 2017	Q
MindPowerSec	BRA	http	██████████.com.br			22 Kasim 2017	Q

10:11 22/11/2017



# CTIR Gov



## Robôs

RB-TWITTER

Pesquisa tweets contendo os domínios e tags pré-definidos, a partir do último id pesquisado.

Utiliza a biblioteca do perl:

Net::Twitter

É possível identificar algumas desfigurações de sítio.

Identifica possíveis preparações para futuros ataques.

É possível acompanhar ataques que estão acontecendo e sendo Relatados no Twitter.



# CTIR Gov

## Robôs



RB-TWITTER

ter, 4 de jul de 2017 11:00:15 Robo-Twitter - Tíquete criado  
Assunto: rb-twitter.pl - [www.xxx.xx.leg.br | 162.xxx.xxx.xxx]  
Para: CTIR Gov <ctir@ctir.gov.br>  
Date: Tue Jul 4 10:00:17 2017  
From: Robo-Twitter <rb-twitter@ctir.gov.br>

Dominio:www.xxx.xx.leg.br

IP: 162.xxx.xxx.xxx

Nr\_URLs:1

1.

URL:http://www.xxx.xx.leg.br/

Motivo:Desfiguracao Twitter

Link do Tweet:twitter.com/VandaTheGod/status/881883334611173378

Data do Tweet:03/07/2017 14:32:26

Data da Triagem:04/07/2017



# CTIR Gov

## Robôs



RB-WEBSITETESTER

Verifica a disponibilidade dos sítios que devem ser monitorados pelo CTIRGov.

Faz 5 tentativas de get nas URLs, caso código da resposta HTTP seja Diferente de 200, cria um Ticket de Indisponibilidade de Sítio.

É útil para identificar ataques de DDoS.



# CTIR Gov Robôs



RB-WEBSITETESTER

qua, 26 de jul de 2017 21:32:31 Robo-Website-Tester - Tíquete criado  
Assunto: rb-website-tester.pl - Erro website - [sistema.xxx.gov.br | 192.xxx.xxx.xxx]  
Para: CTIR Gov <ctir@ctir.gov.br>  
Date: Wed Jul 26 20:32:30 2017  
From: Robo-Website-Tester <rb-website-tester@ctir.gov.br>

1. Ocorreu um erro na resposta HTTP ao acessar:

URL:https://sistema.xxx.gov.br/VOX

Status Line:500 Can't connect to sistema.xxxxo.gov.br:443 (Bad hostname)

=====

2. Dump completo (Status + Cabeçalho + Conteúdo) da resposta HTTP:

Response:

500 Can't connect to sistema.xxx.gov.br:443 (Bad hostname)

Content-Type: text/plain

Client-Date: Wed, 26 Jul 2017 20:32:30 GMT

Client-Warning: Internal response

Can't connect to sistema.xxx.gov.br:443 (Bad hostname)

LWP::Protocol::https::Socket: Bad hostname 'sistema.xxx.gov.br' at  
/opt/rt3/PERL5LIBLocal/LWP/Protocol/http.pm line 51



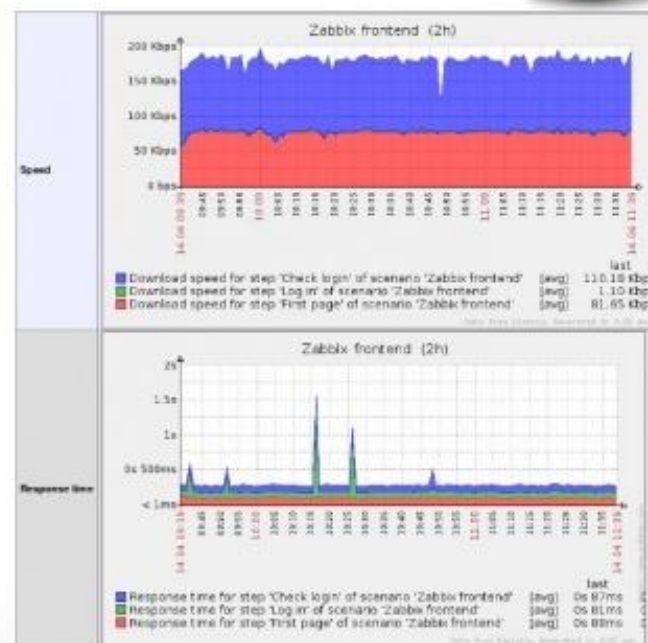
# CTIR Gov ZABBIX



## Monitoramento Web



- Tempo de resposta
- Velocidade de download
- Código de resposta
- Disponibilidade de um determinado conteúdo
- Capacidade para cenários com login/logout
- Suporte a HTTP/HTTPS





# CTIR Gov

## RT

### 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.



# CTIR Gov 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.





# CTIR Gov RT

BEST PRACTICAL™

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

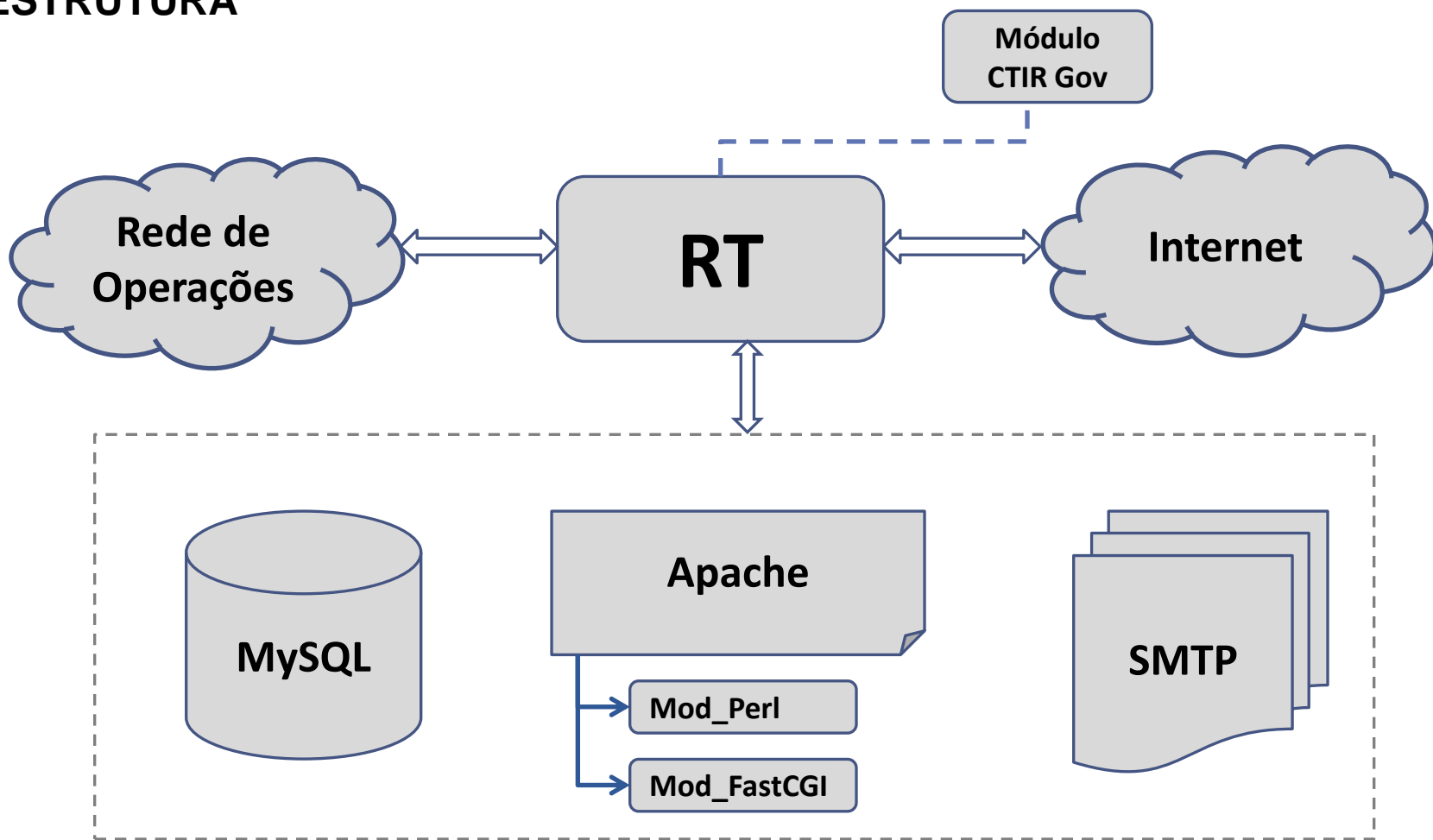




# CTIR Gov RT



## ➤ INFRAESTRUTURA

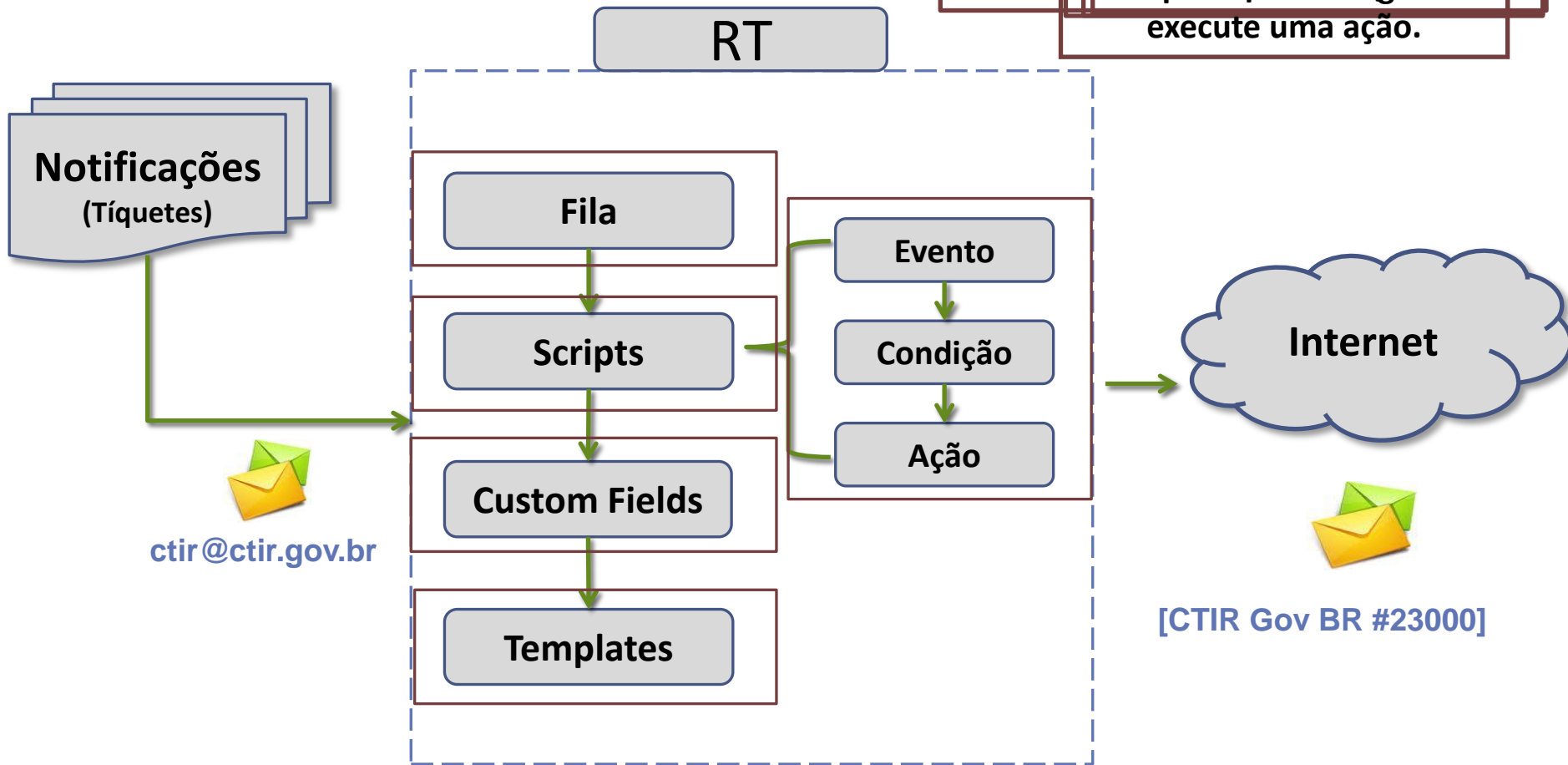




# CTIR Gov

## RT

Trechos de código que são utilizados como componentes do RT são aqueles em que se define uma condição para que seja executada uma ação.



[CTIR Gov BR #23000]



# CTIR Gov RT



## Filas

Administração de filas - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Administração de filas

192.168.206.5/Admin/Queues/index.html

Most Visited ALERTS CSIRTs HACKERS Proxy SandBox Tools Whois RT

### Configuração

- Usuários
- Grupos
- Filas**
- Campos Personalizados
- Global
- Ferramentas
- Preferências
- Aprovação

## Filas Ativas

Selecionar uma fila:

#	Nome	Descrição	Endereço	Prioridade	Padrão	de Vencimento
3	Abuso de Sítio	Comprometimento de sítios da APF	ctir@ctir.gov.br/-	0-0	0	Ativado
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
8	Análise de Malware	Análises de artefatos maliciosos	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
12	Desenvolvimento	Fila para teste de novas Funcionalidades	-/-	0-0	0	Ativado
24	DNS Recursivo	DNS Recursivo aberto	ctir@ctir.gov.br/-	0-0	0	Ativado
27	Error Message	Error Message	ctir@ctir.gov.br/-	0-0	0	Ativado
30	FREAK - Factoring RSA Export Keys	FREAK - Factoring RSA Export Keys	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	ctir@ctir.gov.br/-	0-0	0	Ativado
22	Indisponibilidade de Sítio	Site_Unavailable	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 estatísticas (follow-ups, dfl-cert, respostas automaticas, etc)	ctir@ctir.gov.br/-	0-0	0	Ativado
29	NTP	NTP	ctir@ctir.gov.br/-	0-0	0	Ativado
20	Página Falsa	Sítios falsos de instituições governamentais	ctir@ctir.gov.br/-	0-0	0	Ativado
14	Phishing_Message	Mesagens de phishing tratadas	ctir@ctir.gov.br/-	0-0	0	Ativado
33	RansomWare	RansomWare	-/-	0-0	0	Ativado



# CTIR Gov RT



## Trâmite

#153398: Desfiguração de Sítio [www.sadprev.go.gov.br[216.172.161.81]] - Mozilla Firefox

File Edit View History Bookmarks Tools Help

#153398: Desfiguração de Sítio ...

192.168.206.5/Ticket/Display.html?id=153398

Most Visited ALERTS CSIRTs HACKERS Proxy SandBox Tools Whois RT

seg, 24 de jul de 2017 14:09:29 **The RT System itself - Assunto alterado de 'rb-twitter.pl - [www.sadprev.go.gov.br[216.172.161.81]] para 'Desfiguração de Sítio [www.sadprev.go.gov.br[216.172.161.81]]'**

seg, 24 de jul de 2017 14:09:27 **Mauricio Leite - Estado alterado de 'novo' para 'aberto'**

seg, 24 de jul de 2017 14:09:23 **Mauricio Leite - Estado alterado de 'aberto' para 'novo'**

seg, 24 de jul de 2017 14:08:46 **Mauricio Leite - Estado alterado de 'novo' para 'aberto'**

seg, 24 de jul de 2017 12:55:30 **triagem - Dado a delta**

seg, 24 de jul de 2017 12:39:21 **triagem - Tomado**

seg, 24 de jul de 2017 11:00:15 **The RT System itself - Comentários adicionados** Responder Comentário Reencaminhar Copiar

3 última(s) notificações para [www.sadprev.go.gov.br]:

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

=====

151412 - 27/06/2017 10:00:29 - resolvido - triagem - rb-twitter.pl - [www.sadprev.go.gov.br[216.172.161.81]]

151369 - 26/06/2017 19:50:02 - resolvido - delta - Desfiguração de Sítio [www.sadprev.go.gov.br[216.172.161.81]]

111944 - 16/05/2016 15:03:38 - resolvido - triagem - rb-zone-h.pl - [www.sadprev.go.gov.br[200.98.210.101]]

=====

seg, 24 de jul de 2017 11:00:13 **Robo-Twitter - Tíquete criado** Responder Comentário Reencaminhar Copiar

Assunto: rb-twitter.pl - [www.sadprev.go.gov.br[216.172.161.81]]

Para: CTIR Gov <ctir@ctir.gov.br>

Date: Mon Jul 24 10:00:12 2017

From: Robo-Twitter <rb-twitter@ctir.gov.br>



# CTIR Gov RT



## Scripts

Modificar um scrip para a fila Malware\_Hosting - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Modificar um scrip para a fila Ma... +

192.168.206.5/Admin/Queues/Script.html?id=32&Queue=7

Most Visited ALERTS CSIRTs HACKERS Proxy SandBox Tools Whois RT

RT para CTIR Gov BR Entrou como delta | Preferências | Sair

### Modificar um scrip para a fila Malware\_Hosting

Novo ticket e Abuso de e Buscar...

Selecionar um scrip · Novo scrip · Scrip #32

#### Campos de Scrip

Descrição:

Condição:

Ação:

Modelo:

Estágio:

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 aplicável à ação descrita no Scrip Malware Hosting##
#
# 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";
#####
Condição personalizada: ###-----
## Não satisfaz A NÃO SER que o novo estado seja "Aberto"
return 0 unless $self->TransactionObj->NewValue eq "open";
```



# CTIR Gov RT



## Templates

#153398: Desfiguração de Sítio [www.sadprev.go.gov.br|216.172.161.81] - Mozilla Firefox

File Edit View History Bookmarks Tools Help

#153398: Desfiguração de Sítio ...

192.168.206.5/Ticket/Display.html?id=153398

Most Visited ALERTS CSIRTs HACKERS Proxy SandBox Tools Whois RT

(Mensagem em Português and English version below)

Baixar (sem título) / com cabeçalhos  
text/plain 3k

Prezados Senhores,

1. Informamos a desfiguração do sítio, conforme anexo, em:  
-----  
<http://www.sadprev.go.gov.br/bca.htm>  
-----
2. Sugerimos a correção da vulnerabilidade notificada e 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. 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 Gov <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, do Gabinete de Segurança Institucional 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, ...)



# CTIR Gov RT



## RT-Crontool / Actions

# contem as linhas de comando para rodar as actions da rt-crontool

# Site\_Abuse=3

```
/opt/rt3/bin/rt-crontool --search RT::Search::FromSQL --search-arg "(Status='stalled' AND Queue=3 AND Priority!=75)" --action CtirGov::RT::Action::VerificaDefacement
```

# Malware\_Hosting=7

```
/opt/rt3/bin/rt-crontool --search RT::Search::FromSQL --search-arg "(Status='stalled' AND Queue=7 AND Priority!=75)" --action CtirGov::RT::Action::VerificaMalwareHostingRedirect
```

# Malware\_Redirect=10

```
/opt/rt3/bin/rt-crontool --search RT::Search::FromSQL --search-arg "(Status='stalled' AND Queue=10 AND Priority!=75)" --action CtirGov::RT::Action::VerificaMalwareHostingRedirect
```

# DNS\_Recursivo=24

```
/opt/rt3/bin/rt-crontool --search RT::Search::FromSQL --search-arg "(Status='stalled' AND Queue=24 AND Priority!=75)" --action CtirGov::RT::Action::VerificaDNSRecursivo
```

# PhishingSite=20

```
/opt/rt3/bin/rt-crontool --search RT::Search::FromSQL --search-arg "(Status='stalled' AND Queue='20' AND Priority!=75)" --action CtirGov::RT::Action::VerificaPhishingSite
```

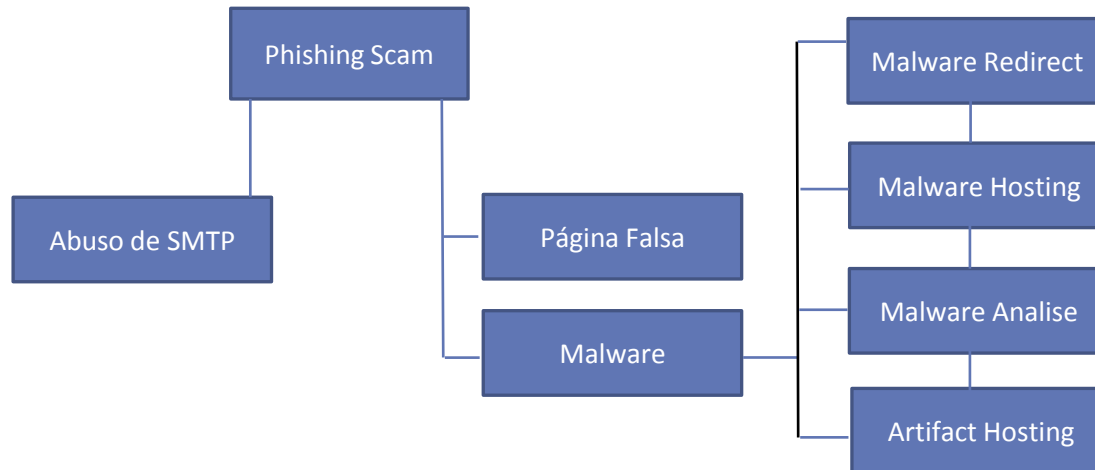




# CTIR Gov RT



## Desdobramento de um Phishing



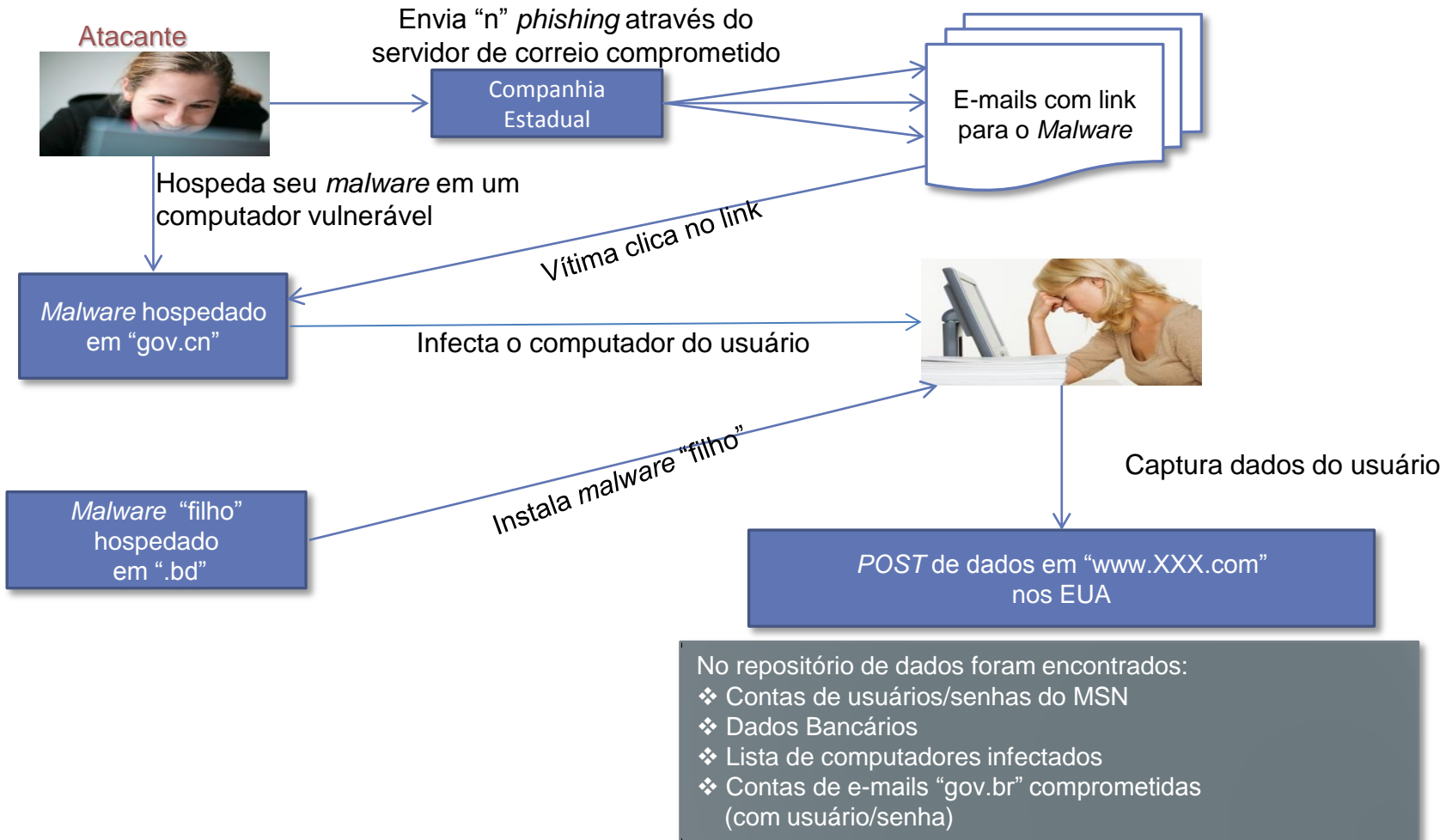


# CTIR Gov RT



## Estudo de Caso

## Engenharia Social (*phishing*) #15327





# CTIR Gov RT



Estudo de Caso

Engenharia Social (*phishing*) #15327

**Vinculos**

Depende de : (Criar)  
 Dependem deste tíquete : (Criar)  
 Pais : (Criar)

## 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]



# CTIR Gov

## DW - Incidentes





# CTIR Gov

## DW - Incidentes

### Modelo Multidimensional BI - CTIR Gov - RT

Dimensão Data
+Id_Data: Numérico
+Id_Trimestre: Numérico
+Descricao_Trimestre: Char
+Id_Ano: Numérico
+Descricao_Ano: Char
+Id_Mes: Numérico
+Descricao_Mes: Char
+Id_Dia: Numérico
+Descricao_Dia: Char

FATO INCIDENTE
ATRIBUTOS
+Id_Ticket: Numérico
+Id_Data: Numérico
+Id_Status: Numérico
+Id_Tipo_Incidente: Numérico
+Id_Local_Destinatario: Numérico
+Id_Local_Origem: Numérico
+Id_Protocolo: Numérico
+Id_Dominio: Numérico
+Id_Analista: Numérico
+Id_Requisitante: Numérico
+Id_Tipo_Site_Abuse: Numérico
+Id_Assunto: Numérico
MÉTRICAS()
+Total de Notificações(): Numérico
+Total de Incidentes(): Numérico
+Total de Incidentes Resolvidos(): Numérico
+Total de Incidentes Pendentes(): Numérico
+Total de Incidentes Não Resolvidos(): Numérico
+Total de Spam(): Numérico
+Total Falso Positivos(): Numérico
+Tempo Trabalhado(): Numérico

Dimensão Status
+Id_Status: Numérico
+Descricao_Status: Char

Dimensão Protocolo
+Id_Protocolo: Numérico
+Descricao_Protocolo: Char

Dimensão Domínio
+Id_Dominio: Numérico
+Descricao_Dominio: Char

Dimensão Usuário
+Id_Usuario: Numérico
+Descricao_Usuario: Char

Dimensão Assunto
+Id_Assunto: Numérico
+Descricao_Assunto: Char

Dimensão Tipo de Incidente
+Id_Tipo_Incidente: Numérico
+Descricao_Tipo_Incidente: Char

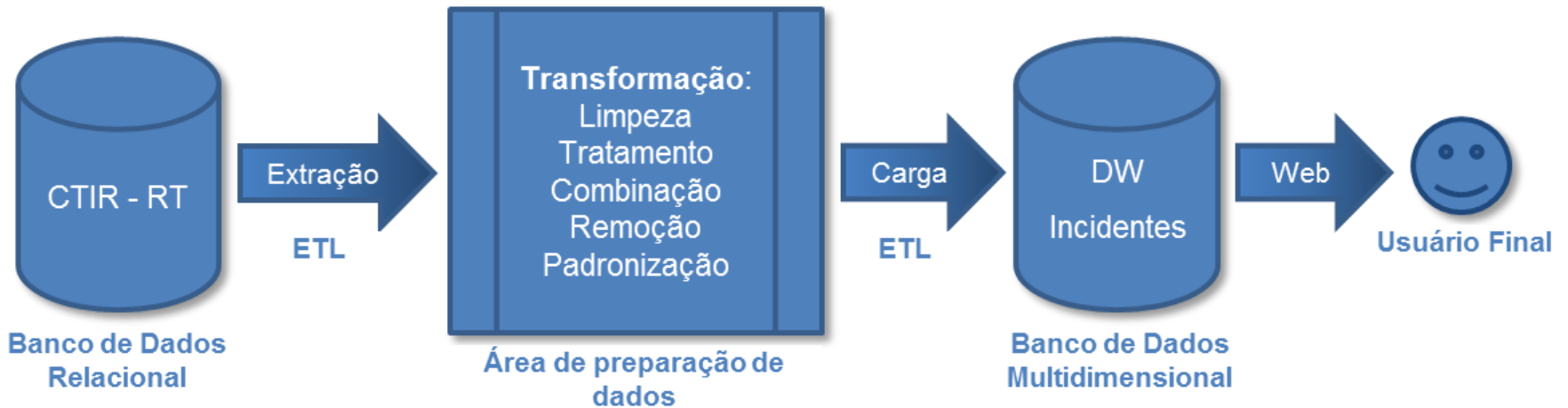
Dimensão Local
+Id_Local: Numérico
+Id_Continente: Numérico
+Descricao_Continente: Char
+Id_Pais: Numérico
+Descricao_Pais: Char
+Id_Regiao: Numérico
+Descricao_Regiao: Char
+Id_Estado: Numérico
+Descricao_Estado: Numérico

Dimensão Tipo de Abuso de Sítio
+Id_Tipo_Site_Abuse: Numérico
+Descricao_Tipo_Site_Abuse: Char



# CTIR Gov

## DW - Incidentes





# CTIR Gov

## DW - Incidentes

1 - Incidentes por Status Mensal - Editor de relatório

Arquivo Editar Exibir Template Filtro Inserir Formato Dados Planilha Mover Janela Ajuda

Salvar e Fechar

Objetos do relatório

Nome	Tipo
Ano	Atributo
Ano Mes	Atributo
Ano Semestre	Atributo
Ano Trimestre	Atributo
Grupo de Incidentes_Status	Grupo Personalizado
QTD_Tickets_Todos	Métrica

Detalhes do Relatório

Filtro do relatório:  
Filtro vazio

Limite do relatório:  
Filtro vazio

Cache de Relatório Utilizado: Não

Filtro de relatório: 'Filtro local'

Clique duas vezes aqui para adicionar uma qualificação ou arraste um objeto do navegador de objetos.

Visualização de relatório: 'Template local' Alternar para:

Ano Ano Semestre Ano Trimestre

Métricas	Ano Mes	Grupo de Incidentes_Status
QTD_Tickets_Todos		

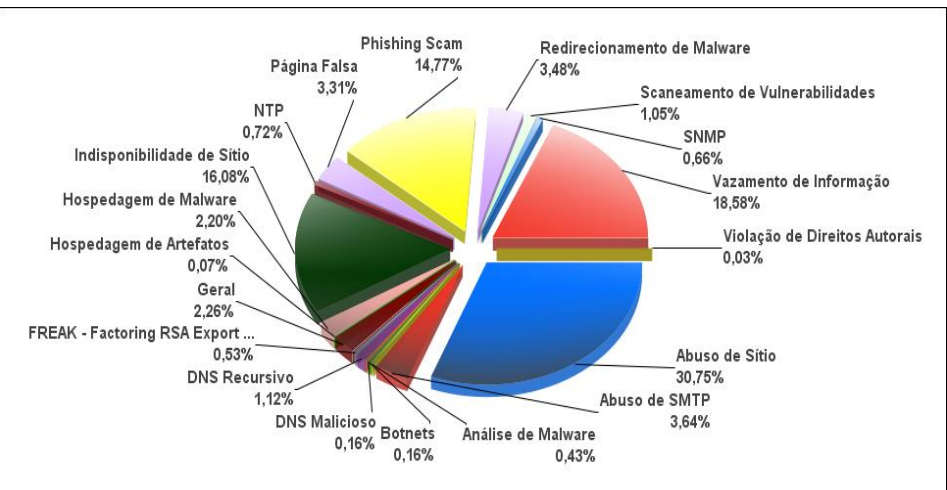
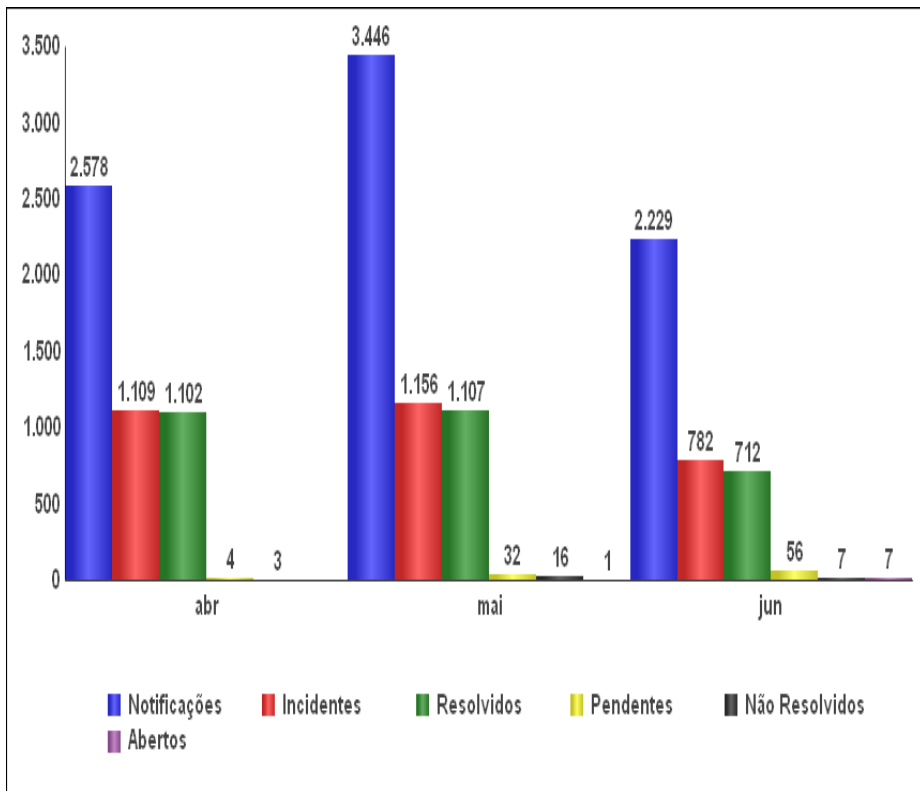
Localizar:

Filtro local Template local Padrão



# CTIR Gov

## DW - Incidentes



Fila	Incidentes
Abuso de Sítio	937
Abuso de SMTP	111
Análise de Malware	13
Botnets	5
DNS Malicioso	5
DNS Recursivo	34
FREAK - Factoring RSA Export Keys	16
General	69
Hospedagem de Artefatos	2
Hospedagem de Malware	67
Indisponibilidade de Sítio	490
NTP	22
Página Falsa	101
Phishing Scam	450
Redirecionamento de Malware	106
Scaneamento de Vulnerabilidades	32
SNMP	20
Vazamento de Informação	566
Violação de Direitos Autorais	1

Ano Mes	Notificações	Incidentes	Resolvidos	Pendentes	Não Resolvidos	Abertos
abr	2.578	1.109	1.102	4	3	
mai	3.446	1.156	1.107	32	16	1
jun	2.229	782	712	56	7	7
<b>Total</b>	<b>8.253</b>	<b>3.047</b>	<b>2.921</b>	<b>92</b>	<b>26</b>	<b>8</b>





# CTIR Gov



## Demonstrativo de Incidentes tratados pelo CTIR Gov no período de 2013 a 2017

Fila	2013	2014	2015	2016	2017	TOTAL	
Abuso de Sítio	1.673	1.831	2.337	2.807	2.217	10.865	←
Abuso de SMTP	1.101	838	696	1.011	324	3.970	←
Análise de Malware	447	439	386	344	46	1.662	
Botnets	8	99	122	108	19	356	
DNS Malicioso	0	62	169	5	1	237	
DNS Recursivo	143	7	15	115	17	297	
FREAK - Factoring RSA Export Keys	0	0	0	23	137	160	
Geral	73	36	43	63	299	514	
Hospedagem de Artefatos	52	97	60	43	132	384	
Hospedagem de Malware	657	725	536	312	3	2.233	
Indisponibilidade de Sítio	1.347	1.309	967	1.863	162	5.648	←
NTP	0	0	0	105	1.357	1.462	
Página Falsa	582	1.278	1.570	1.244	61	4.735	←
Phishing Scam	1.470	1.275	1.441	1.336	265	5.787	←
QOTD	0	0	0	0	714	714	
RansomWare	0	0	0	0	1	1	
Redirecionamento de Malware	454	812	407	400	15	2.088	
Scaneamento de Vulnerabilidades	723	369	358	347	296	2.093	
Transferência de Zona DNS	0	0	47	0	94	141	
SNMP	0	0	0	58	51	109	
Vazamento de Informação	110	400	333	2.044	797	3.684	
Violação de Direitos Autorais	0	8	5	8	2	23	
<b>TOTAL</b>	<b>8.840</b>	<b>9.585</b> ←	<b>9.492</b>	<b>12.236</b> ←	<b>7.010</b>	<b>47.163</b>	



# 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.

<http://www.cert.org/>



# CTIR Gov



## OBRIGADO!

Maurício Leite Ferreira da Silva

[mauricio.leite@presidencia.gov.br](mailto:mauricio.leite@presidencia.gov.br)

61 - 3411-2308

<http://www.ctir.gov.br>

[ctir@ctir.gov.br](mailto:ctir@ctir.gov.br) (notificação de incidentes)

INOC-DBA: **10954\*810**

