



INTRAREDE 2022

Como se prevenir e atuar durante um incidente de segurança

Ricardo Kléber M. Galvão

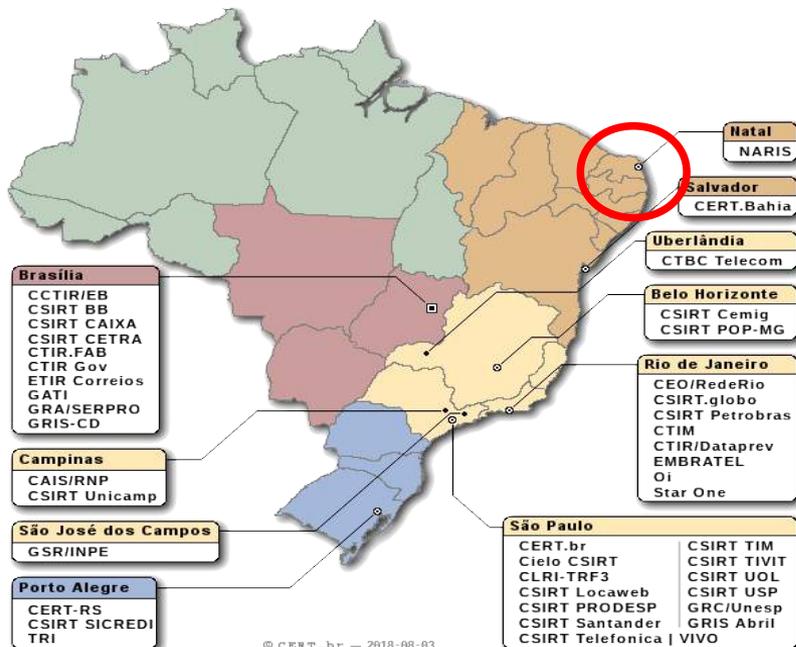
ricardokleber@ricardokleber.com.br



Contextualização

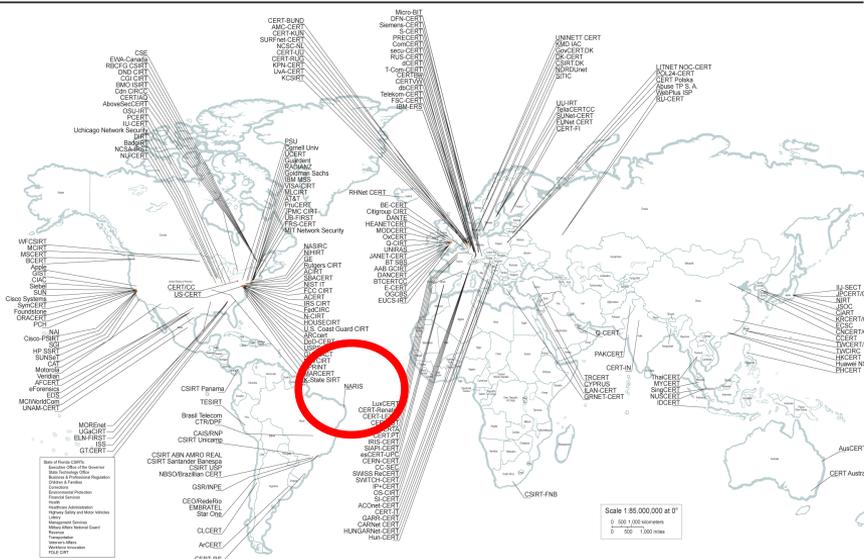


Colocando o “NARIS” onde não era chamado (mas que precisava embora não percebesse)



Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.





QUALQUER instituição sem um CSIRT...



Apagar Incêndios

**Enquanto ainda
há o que apagar...**





Provocação necessária

Questão de maior relevância na atualidade...

SE vou sofrer um
(grave) Incidente de Segurança





Provocação necessária

Quando!!!

~~SE~~ vou sofrer um
(grave) Incidente de Segurança



*Estou preparado?
Sobreviverei?*



Não é terrorismo!!!



<https://exame.com/negocios/ataques-de-hacker-perdas-de-us-280-bi-para-empresas/>

<https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml>

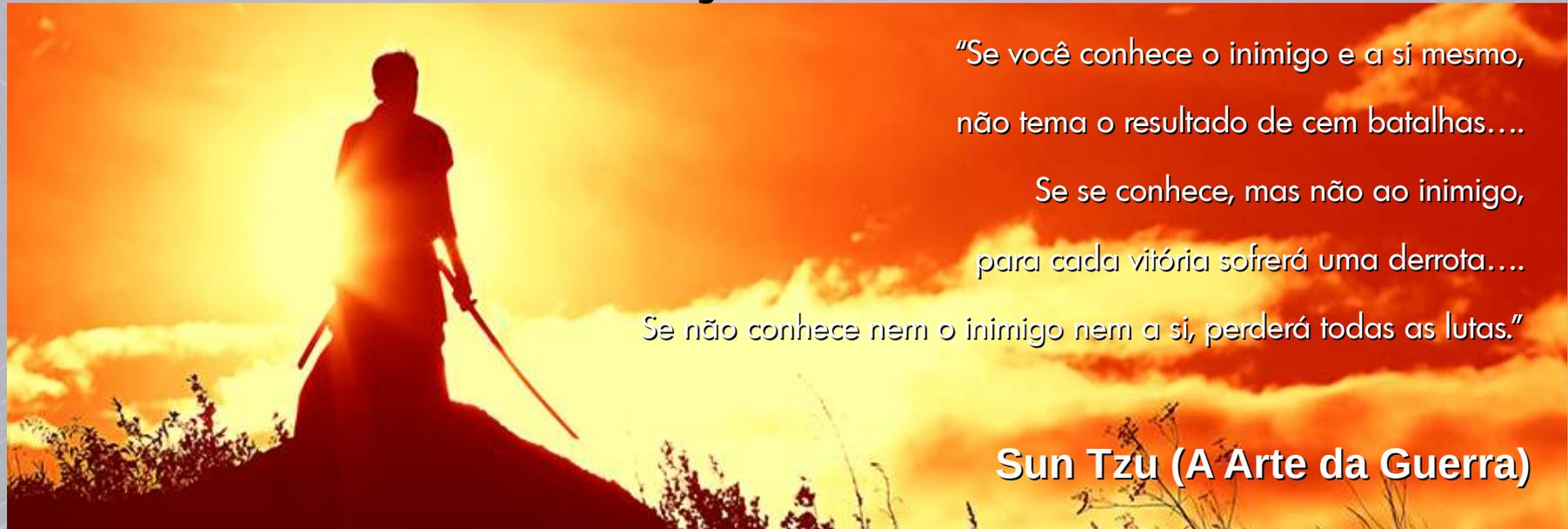


Palavras de "Ordem"

Proatividade

Cooperação

Capacitação (Contínua)



"Se você conhece o inimigo e a si mesmo,
não tema o resultado de cem batalhas....

Se se conhece, mas não ao inimigo,
para cada vitória sofrerá uma derrota....

Se não conhece nem o inimigo nem a si, perderá todas as lutas."

Sun Tzu (A Arte da Guerra)



Motivação

- Aumento generalizado na quantidade e diversidade de incidentes de segurança;
- Aumento generalizado na quantidade e variedade de organizações sendo afetadas por incidentes de segurança em sistemas computacionais;
- Maior consciência, por parte das organizações, da necessidade de políticas e práticas de segurança como parte das suas estratégias globais de gerenciamento de riscos;
- Novas leis e regulamentos que afetam a maneira como as organizações precisam proteger as suas informações; e
- Percepção de que administradores de redes e sistemas não podem proteger sozinhos os sistemas e as informações da organização.



O que (tentar) fazer (com ou sem equipe)

- Criação de ponto (único) de contato na rede para comunicar problemas de segurança;
- Disponibilidade (efetiva) para classificar e atuar prontamente no caso de incidentes;
- Estabelecimento/utilização de normas/padrões específicas para incidentes;
- Tratamento de notificações externas encaminhadas à instituição;
- Identificação e tratamento de incidentes internos na instituição;
- Notificação de incidentes a outros grupos (externos à instituição);
- Monitoramento contínuo de ambiente computacional (interno e externo).





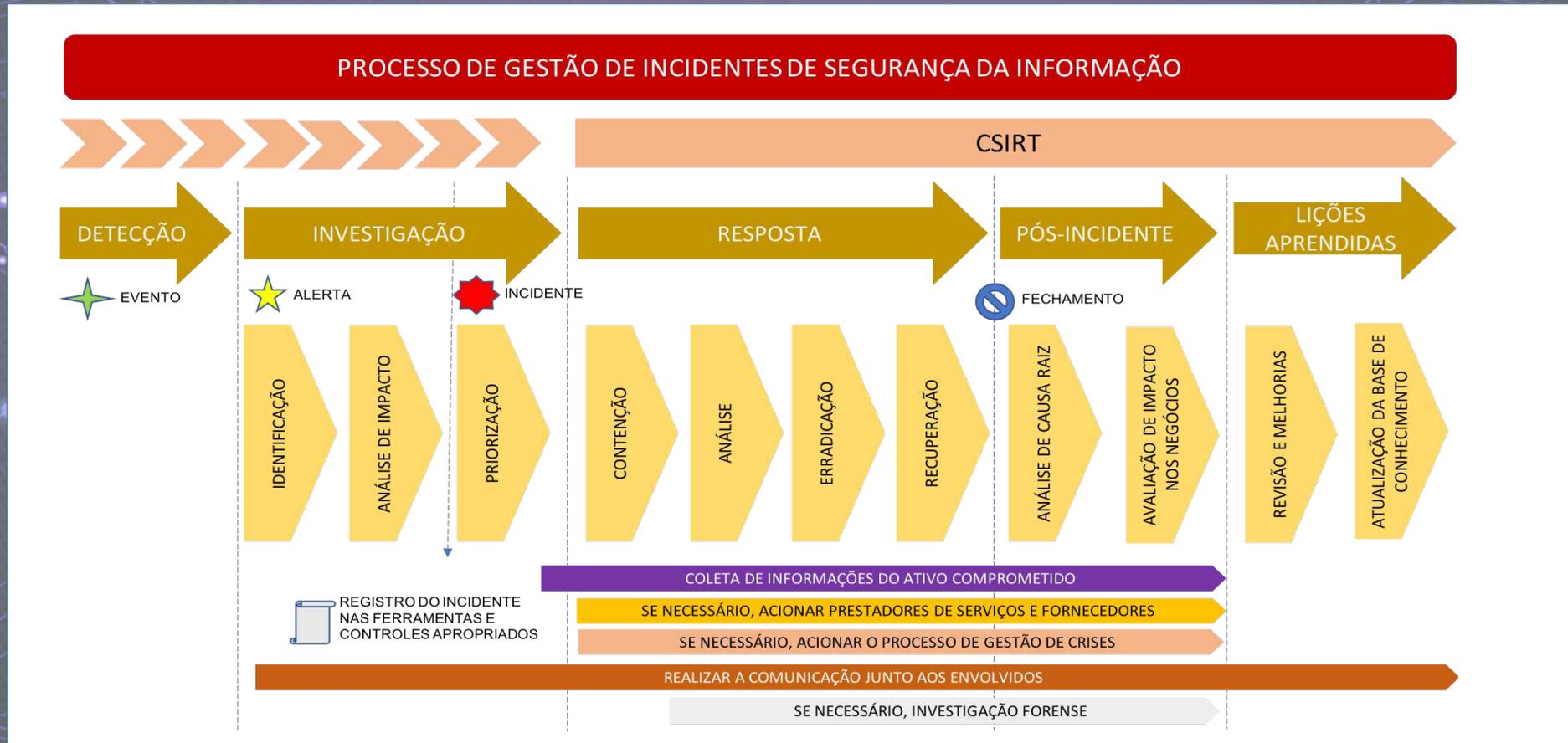
Ações Contínuas

- Resposta a incidentes (notificações externas) e notificação de incidentes (incidentes internos);
- Atendimento a demandas internas (clientes/setores);
- Instalação, manutenção e monitoramento de mecanismos de segurança (Firewalls, IDS, LogHosts);
- Análise de vulnerabilidades e avaliações (periódicas) de segurança;
- Atenção e Emissão de alertas e advertências;
- Prospecção e/ou monitoramento de novas tecnologias;
- Desenvolvimento/adaptação de ferramentas de segurança;
- Disseminação de informações relacionadas à segurança.





Atuação proativa em incidentes





Documentação/Normas

- [RFC 2350] Expectations for Computer Security Incident Response
 - <https://www.ietf.org/rfc/rfc2350.txt>
- [RFC 2196] Site Security Handbook
 - <https://www.ietf.org/rfc/rfc2196.txt>



Melhor fonte de apoio (em português)

The screenshot shows a web browser window with the URL cert.br/csirts/brasil/. The page is titled "Núcleo de Informação e Coordenação do Ponto BR" and contains the following content:

- Navigation links: [CGI.br](#), [NIC.br](#), [Registro.br](#), [CERT.br](#), [CETIC.br](#), [CEPTRO.br](#), [W3C.br](#)
- Breadcrumbs: Você está em: [CERT.br](#) > [CSIRTs](#) > [CSIRTs Brasileiros](#)
- Section: **Grupos de Segurança e Resposta a Incidentes (CSIRTs) Brasileiros**
- Text: Esta página contém informações sobre Grupos de Segurança e Resposta a Incidentes (CSIRTs) brasileiros. Para que um time esteja listado nesta página ele precisa atender aos seguintes requisitos:
 - Estar operacional há pelo menos 6 meses;
 - Ser reconhecido por sua organização ou público alvo;
 - Ter preenchido os requisitos do **formulário de solicitação de inclusão**;
 - Identificar dois times, seus *sponsors*, que estejam listados nesta página e que possam atestar a veracidade dos itens anteriores;
 - Responder periodicamente os testes de reação que são enviados para o endereço de *e-mail* informado como contato para notificação de incidentes.
- Text: Se você for membro de um Grupo que não esteja listado aqui, por favor utilize o **formulário para solicitar a inclusão**.
- Section: **Informações de Contato de CSIRTs Brasileiros**
- Text: A seguir são listadas, em ordem alfabética dos acrônimos, as informações de contato de cada um dos grupos.
- Section: **CAIS/RNP — Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa**
- Text:
 - Redes Atendidas:** Instituições de ensino superior, institutos de pesquisa e similares, conectados ao backbone da RNP.
 - E-mail:** cais@cais.rnp.br
 - INOC-DBA:** 1916*800
 - Sede:** Campinas – SP
 - Chave PGP**
 - Filiações:**
 - FIRST Full Member

<https://www.cert.br/csirts/brasil/>

Ricardo Haber



Fala que eu te escuto...

- www.ricardokleber.com.br
- ricardokleber@ricardokleber.com.br
- [@ricardokleberoficial](https://www.instagram.com/ricardokleberoficial)
- [youtube.com/segurancaderedes](https://www.youtube.com/segurancaderedes)
- [youtube.com/rkifrnccn](https://www.youtube.com/rkifrnccn)
- [youtube.com/ricardokleber](https://www.youtube.com/ricardokleber)

