INTRAREDE
2022

Como se prevenir e atuar durante um incidente de segurança

Ricardo Kléber M. Galvão

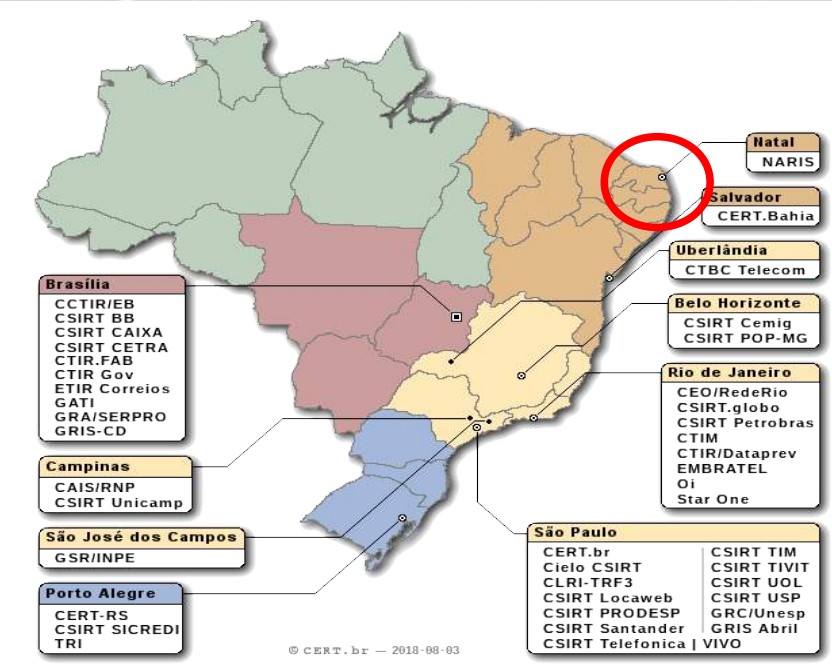
ricardokleber@ricardokleber.com..br

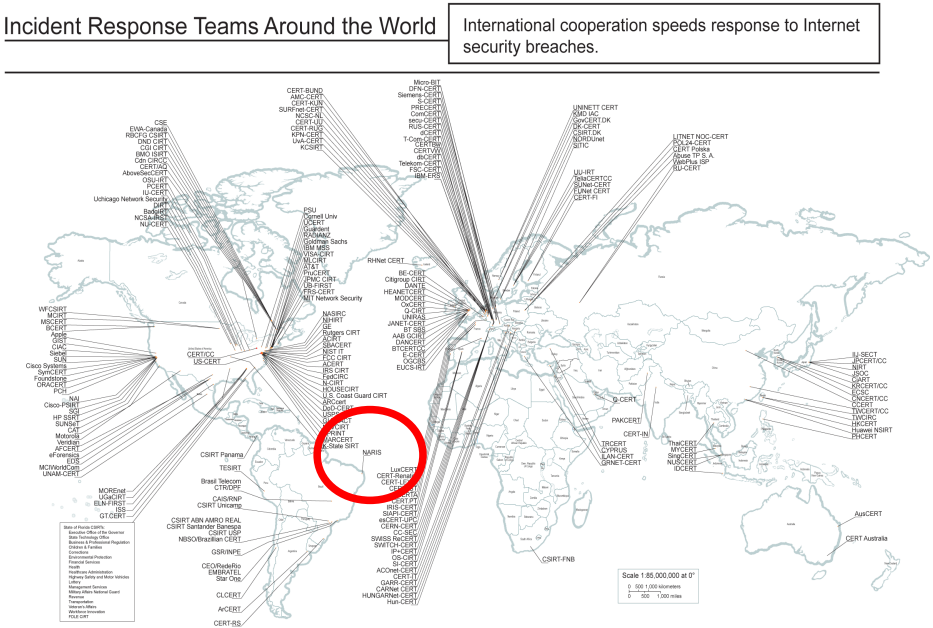
13/07/2022

Contextualização

NARIS
NÚCLEO DE ATENDIMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA

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





Ricardo Kléber

QUALQUER instituição sem um CSIRT...

Apagar Incêndios

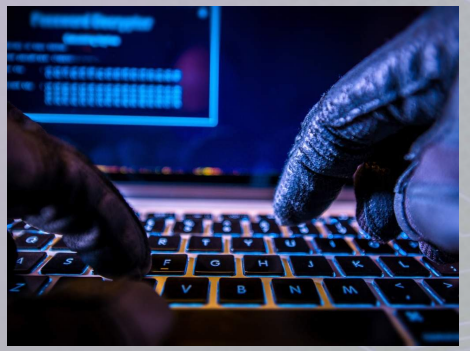
Enquanto ainda
há o que apagar....

Ricardo Kléber

Provocação necessária

Questão de maior relevância na atualidade...

SE vou sofrer um (grave) Incidente de Segurança



Ricardo Kléber

Provocação necessária

Quando!!!

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

Estou preparado?
Sobreviverei?

Ricardo Kléber

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

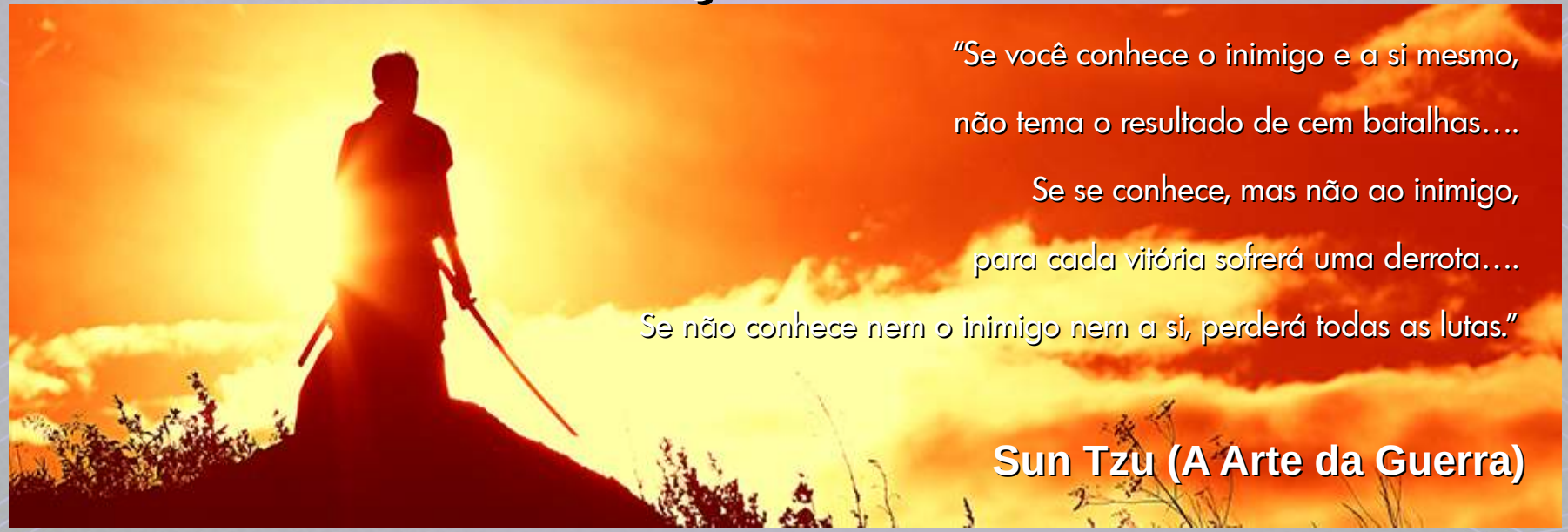
Ricardo Kleber

Palavras de "Ordem"

Proatividade

Cooperação

Capacitação (Contínua)



Ricardo Kléber

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.

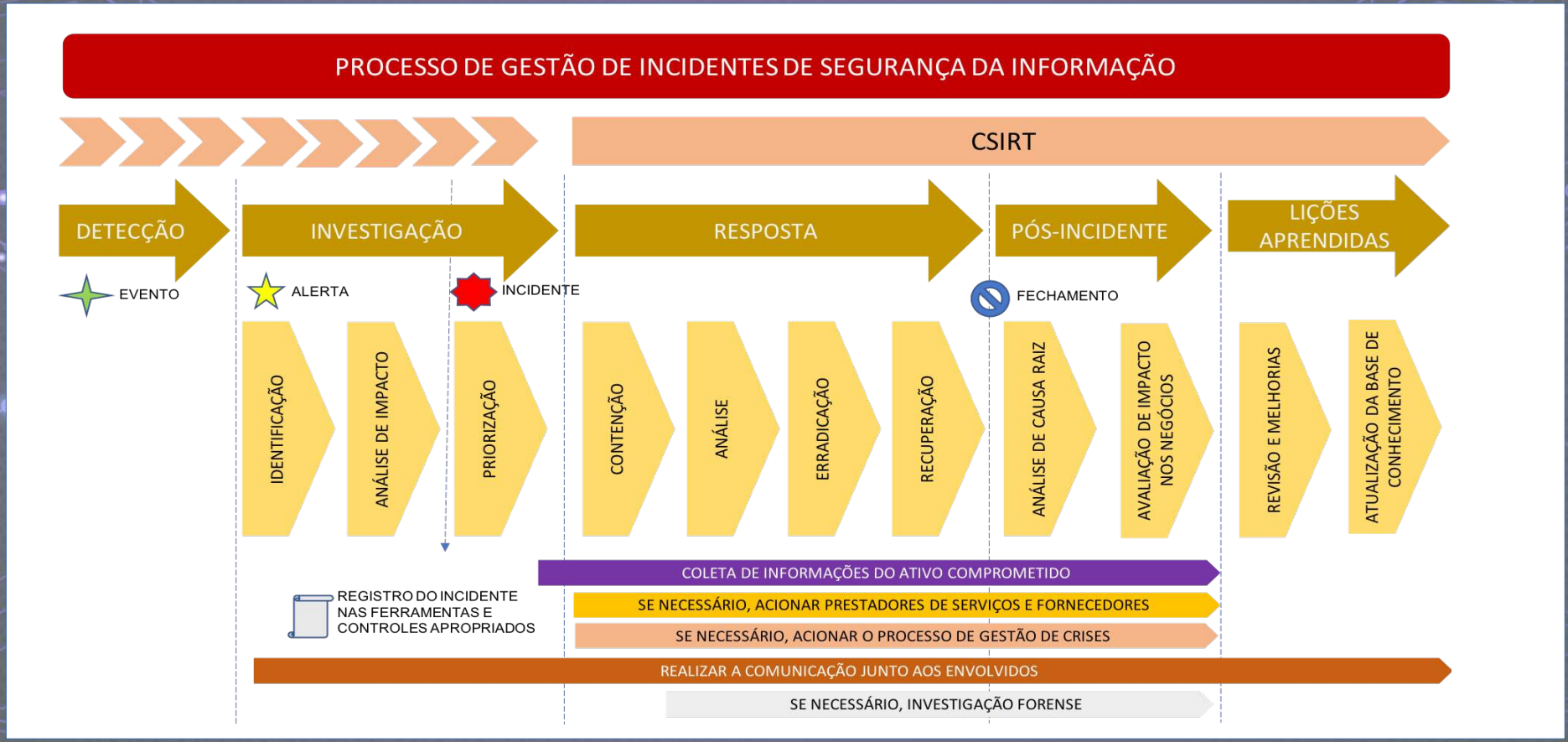
O que (tentar) fazer (com ou sem equipe)

- 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);
- Instação, 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.

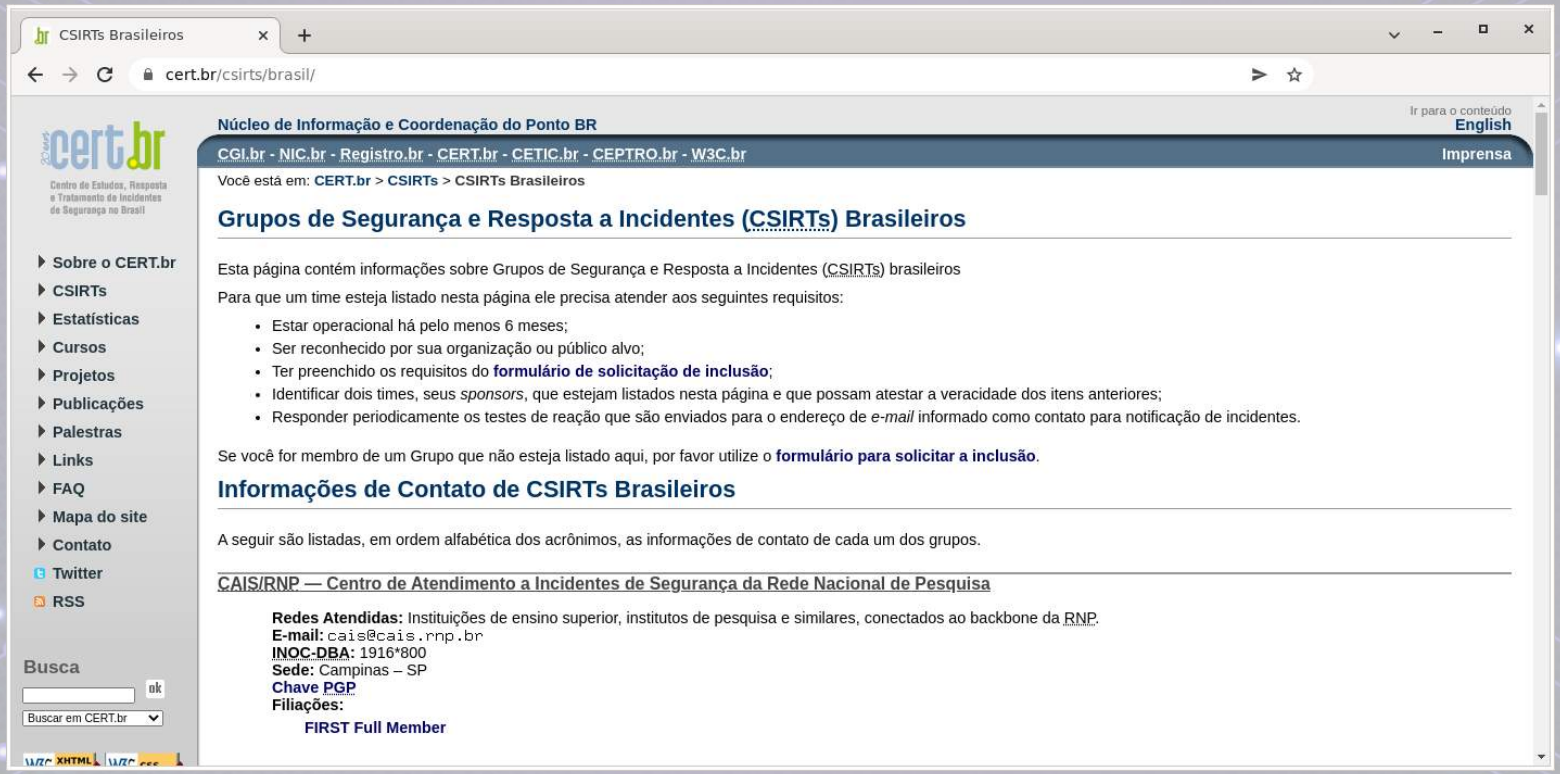
Atuação proativa em incidentes



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)



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

Ricardo Kleber

Fala que eu te escuto...

- www.ricardokleber.com.br
- ricardokleber@ricardokleber.com.br
- @ricardokleberoficial
- youtube.com/segurancaderedes
- youtube.com/rkifrncn
- youtube.com/ricardokleber