nic.br cgi.br | cert.br

A conformidade do Poder Judiciário à Lei Geral de Proteção de Dados – Desafios técnicos e jurídicos sobre privacidade e proteção de dados pessoais no TJSP

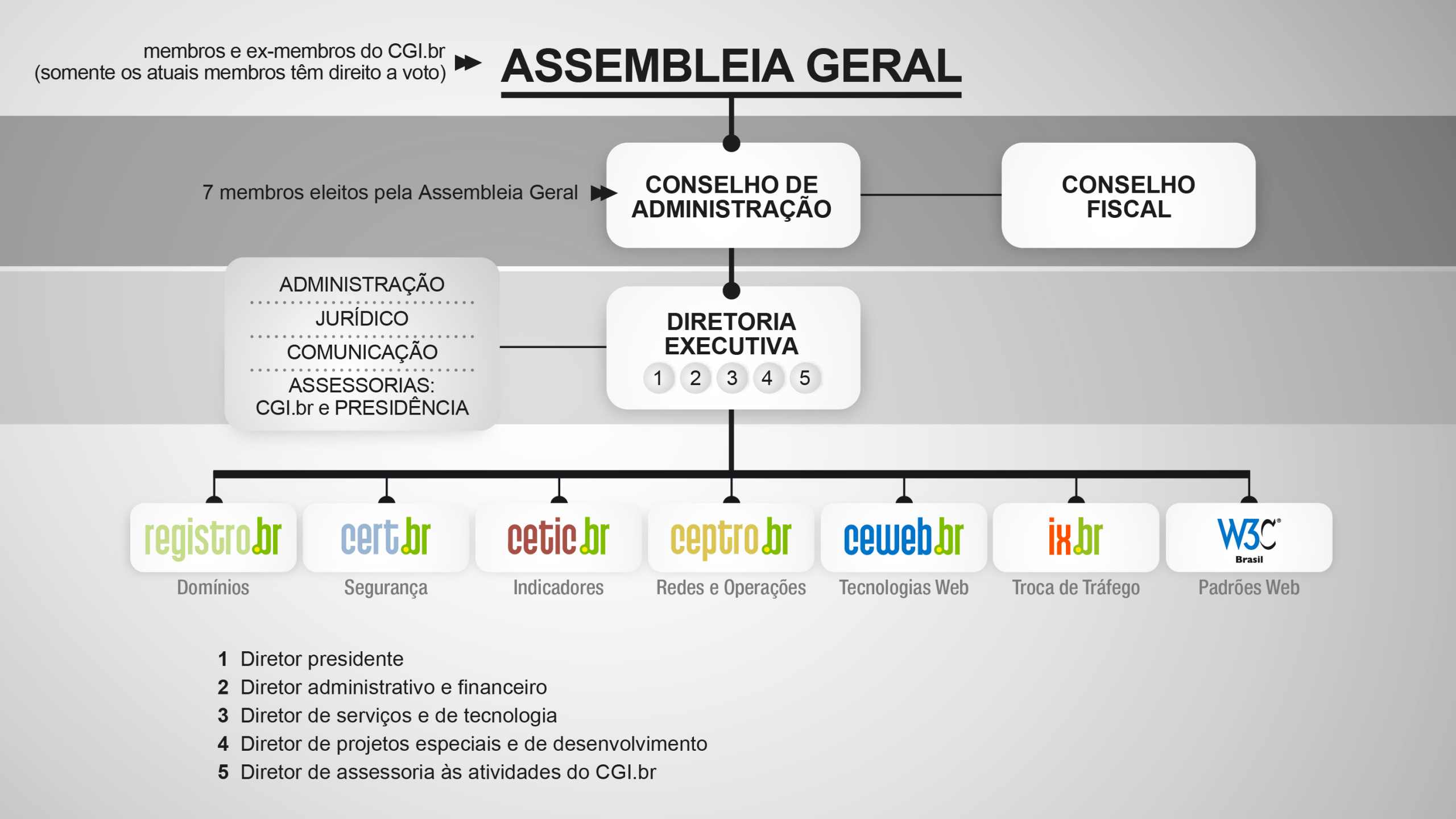
São Paulo, SP | 25/04/2019

Estruturando um plano de governança de dados II:

Como construir e adequar uma política de segurança da informação e gerenciar incidentes de segurança?

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

cert.br nic.br cgi.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

CERT.br:
Estrutura e Serviços

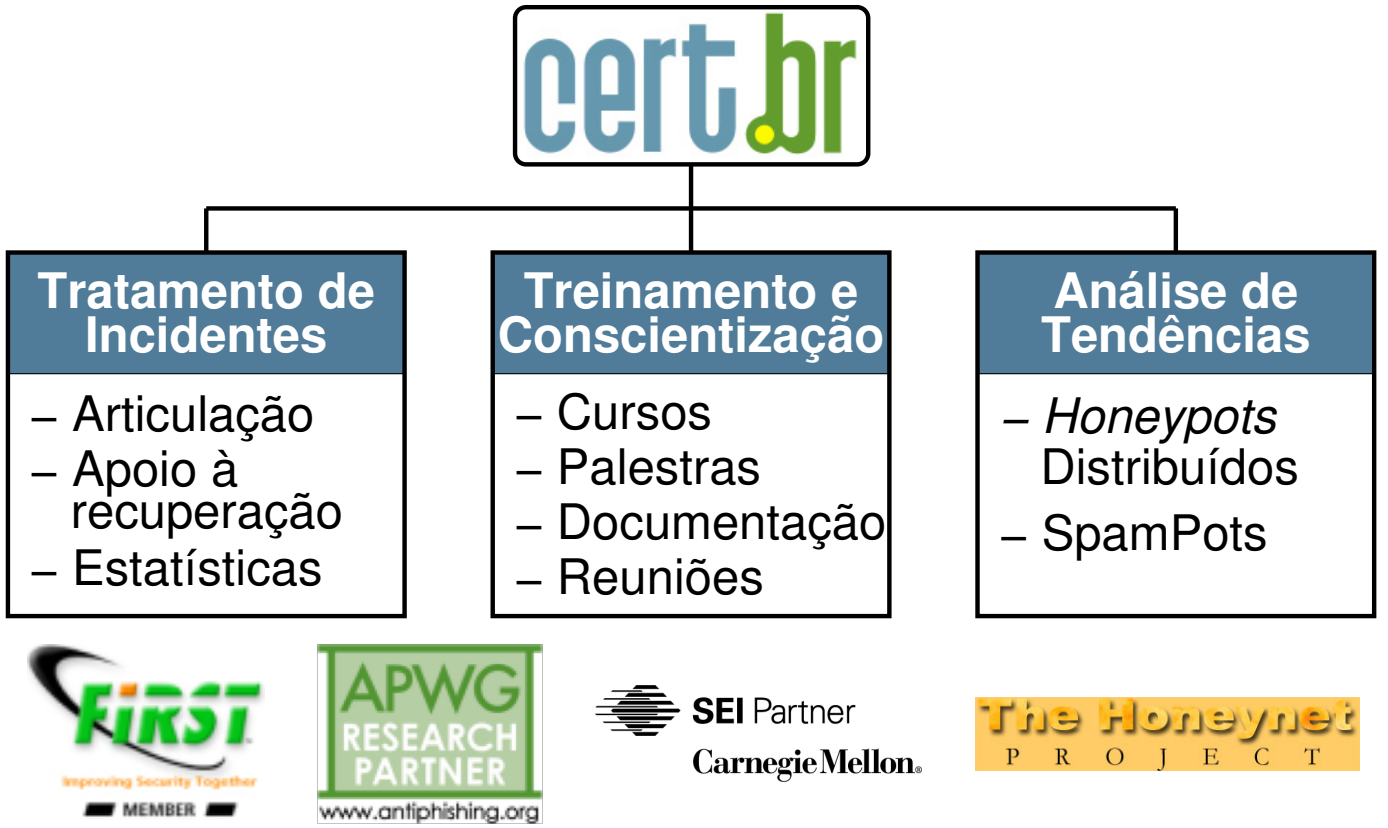
Principais atividades:

Tratamento de Incidentes

- Ponto de contato nacional para notificação de incidentes
- Atua facilitando o processo de resposta a incidentes das várias organizações
- Trabalha em colaboração com outras entidades
- Auxilia novos CSIRTs a estabelecerem suas atividades

Formação de profissionais para atuar em Tratamento de Incidentes

Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências



Criado em 1997 por decisão do CGI.br:

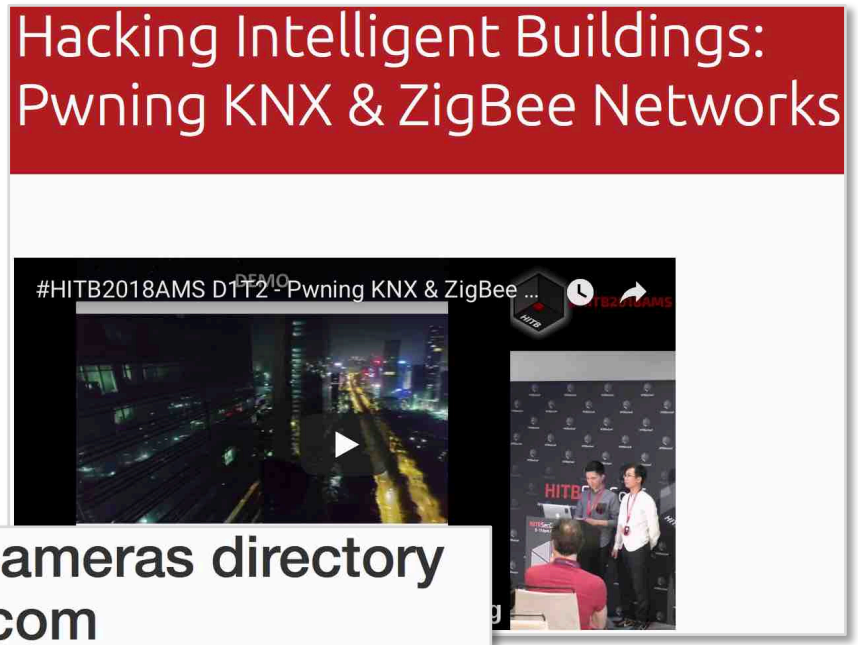
Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional

É Possível Segurança 100%?

Slides disponíveis em:
https://cert.br/docs/palestras/

cert.br nic.br cgi.br



https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs
https://wjla.com/news/local/officials-dc-security-cameras-hacked-8-days-before-inauguration-by-man-woman-in-london
https://conference.hitb.org/hitbsecconf2018ams/sessions/hacking-intelligent-buildings-pwning-knx-zigbee-networks/
http://www.insecam.org

Exemplos Concretos da Dificuldade de Impedir a Invasão de Sistemas

- Comprometimento da RSA/EMC, para furto de material criptográfico – levou ao comprometimento do DoD (*US Department of Defense*)
  https://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex991.htm

- Comprometimento do *Office of Personnel Management*, para furto dos antecedentes de todos os funcionários do Governo Americano
  https://www.opm.gov/cybersecurity/cybersecurity-incidents

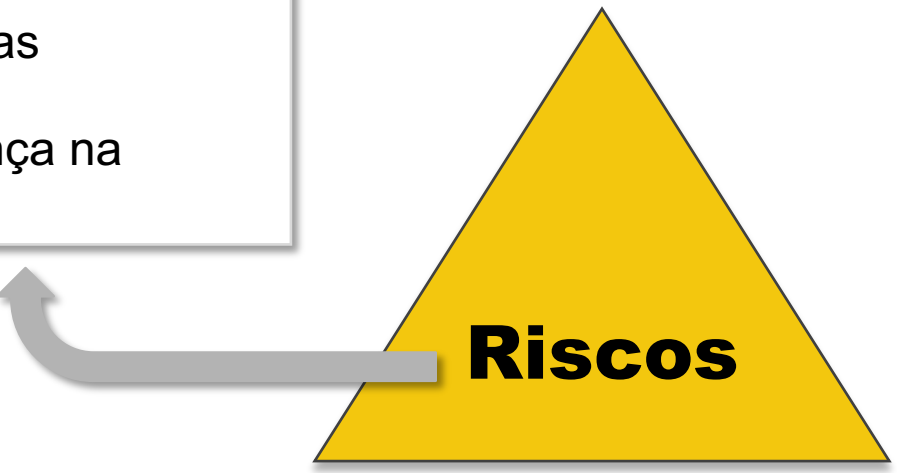
- Comprometimento da Autoridade Certificadora da Holanda – usada para gerar chaves falsas do Google, usadas em espionagem no Irã
  http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html

Segurança, Resiliência e Gestão de Incidentes

cert.br nic.br cgi.br

Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- **perda de privacidade**
- **furto de dados**
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia



- criminosos
- espionagem industrial
- governos
- vândalos

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Propriedades da Segurança da Informação

Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

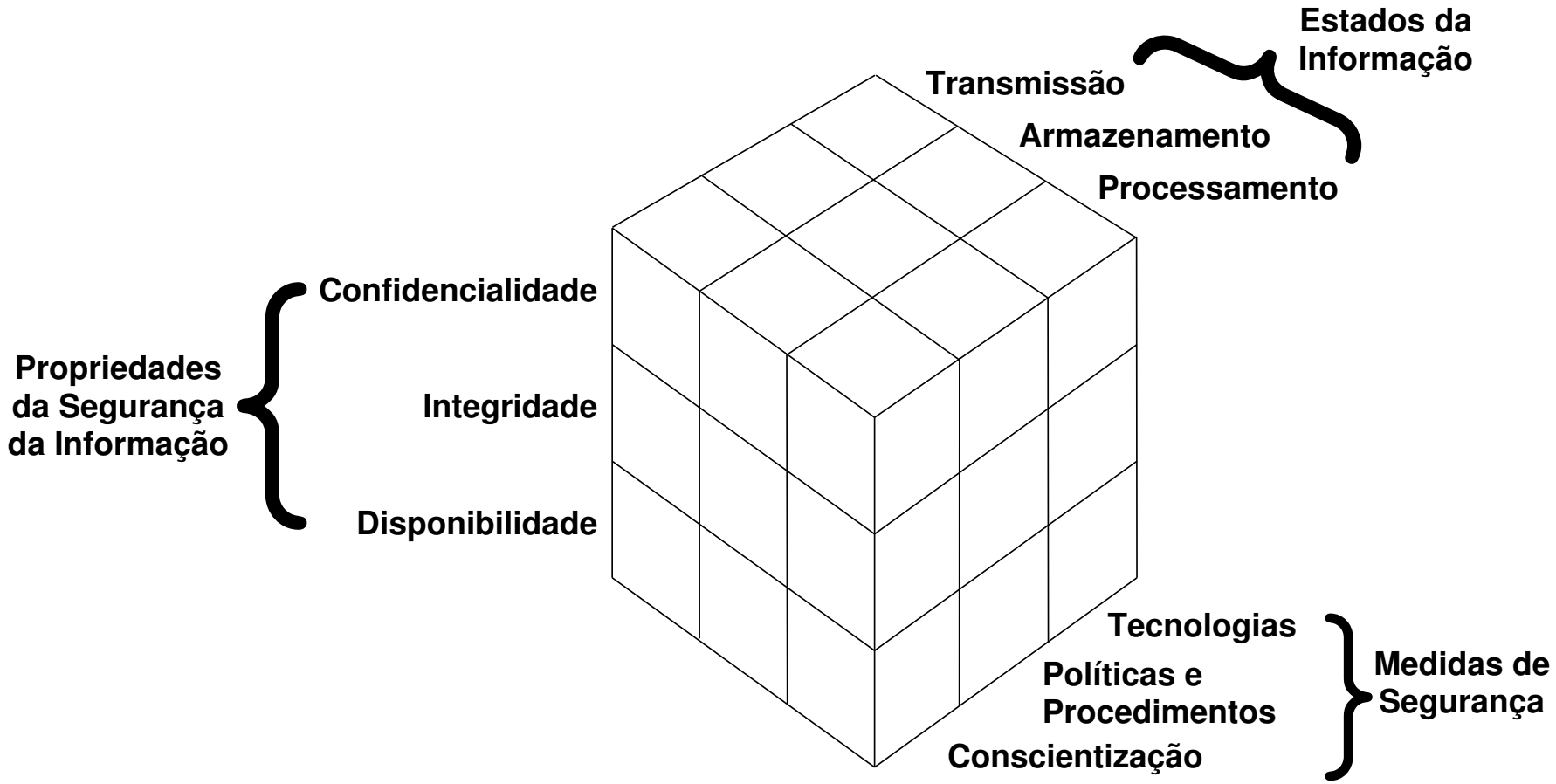
Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

Os dados e as informações estão em diversos locais e a segurança (proteção) depende de múltiplos fatores



McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

Organizações Precisam Almejar Resiliência

Um sistema 100% seguro é muito difícil de atingir

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

- **Identificar o que é crítico** e precisa ser mais protegido (Análise de Risco)
- **Definir políticas** (de uso aceitável, acesso, segurança, etc)
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- **Implantar medidas de segurança** que implementem as políticas de segurança
  - como: aplicar correções ou instalar ferramentas de segurança
- Formular **estratégias e processos para gestão de incidentes** de segurança e formalizar **grupos de tratamento de incidentes (CSIRTs)**

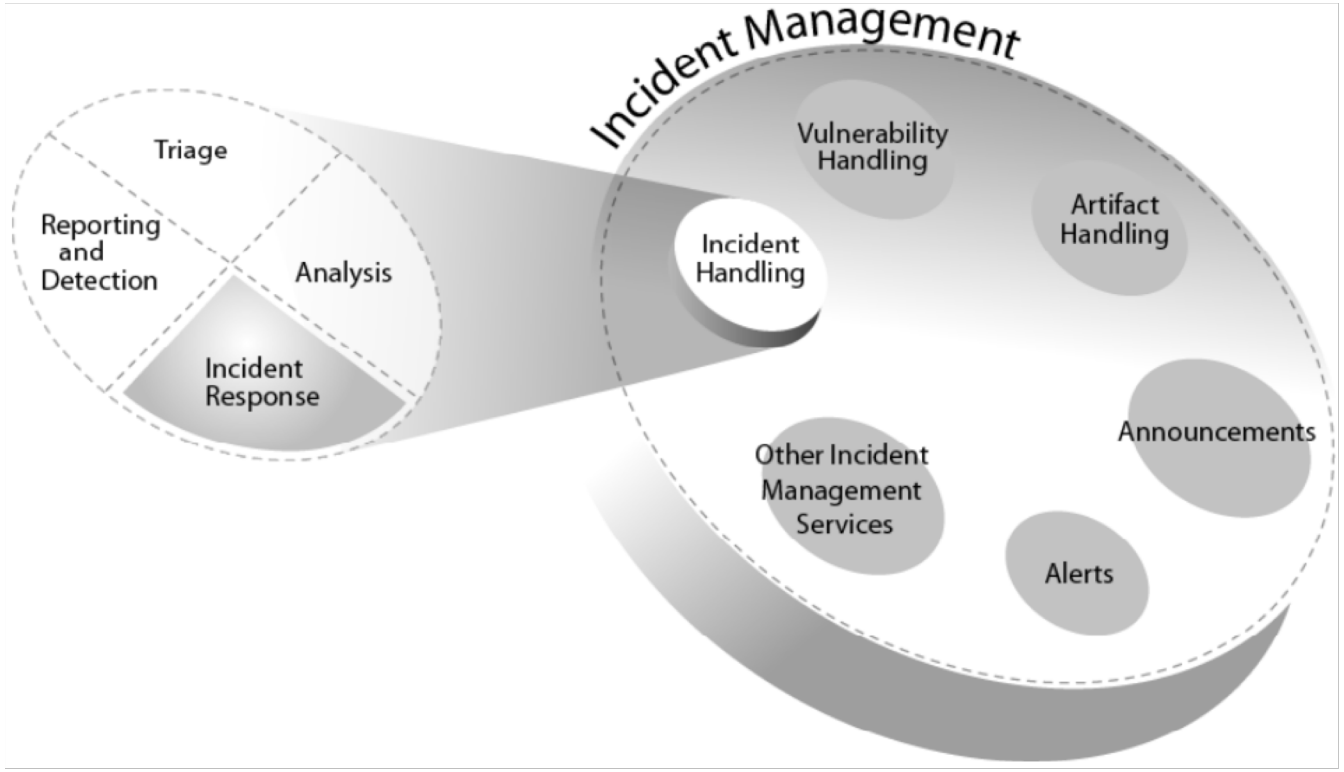
Conceitos Relacionados a Gestão de Incidentes

Incidente de Segurança em Computadores – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

Gestão de Incidentes – capacidade de prover a gestão fim a fim de eventos e incidentes de segurança que afetem ativos de TI e Informação em toda a organização

Tratamento de Incidentes – processo de identificar, mitigar e prevenir incidentes de segurança

Resposta a Incidentes – ações tomadas para resolver ou mitigar incidentes, disseminar informações e implementar estratégias para impedir que o incidente ocorra novamente



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*****. Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Processos de Gestão e Tratamento de Incidentes

Proteção da infraestrutura

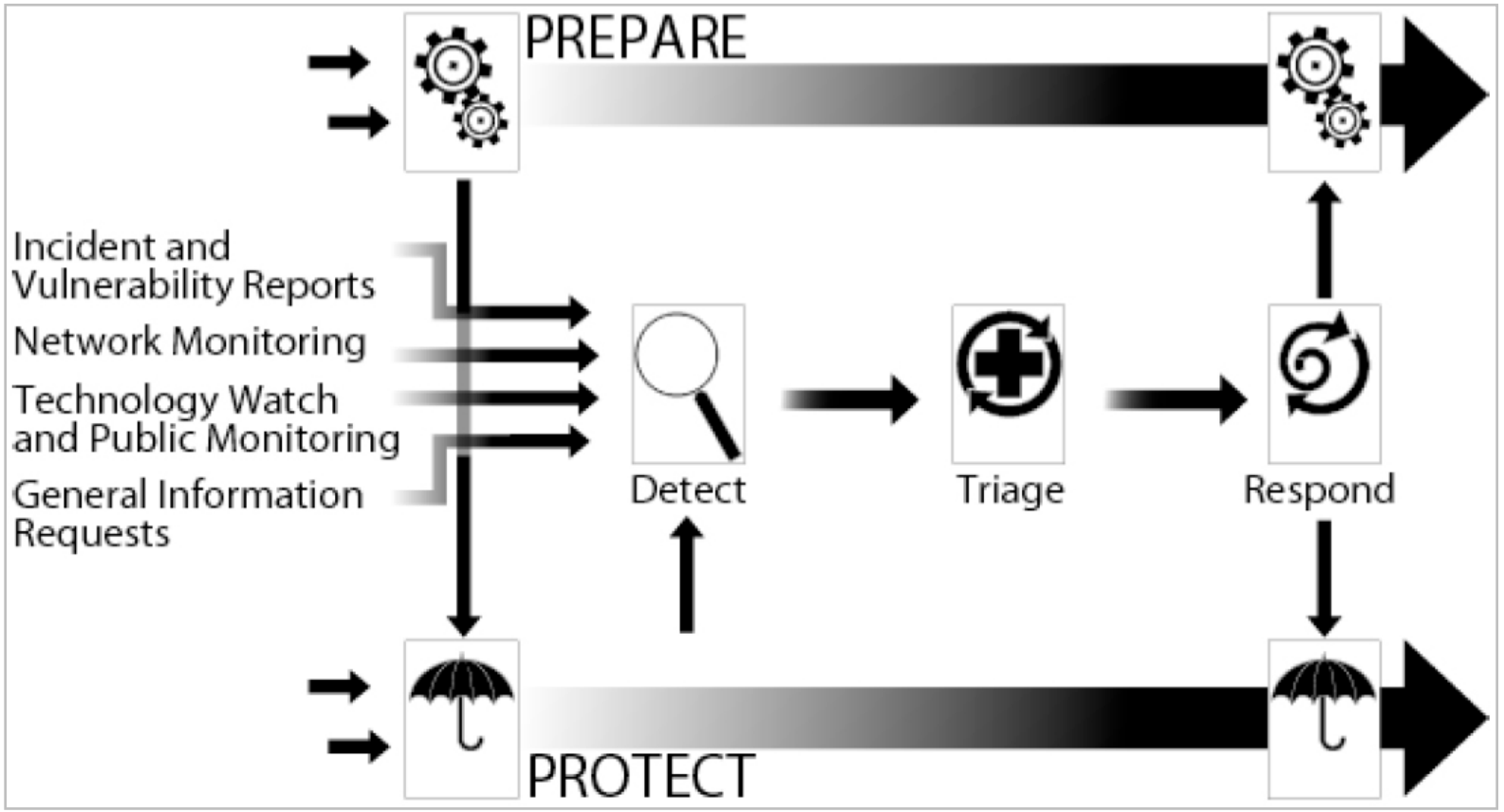
- processo contínuo de implementação de medidas de segurança

Preparação da organização

- educar a organização para a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT

Tratamento de incidentes

- recebe informações de, e alimenta os outros processos
- depende de integração com todas as áreas e alta qualificação das equipes



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*****. Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Integração entre Diversas Áreas

Gestão de incidentes

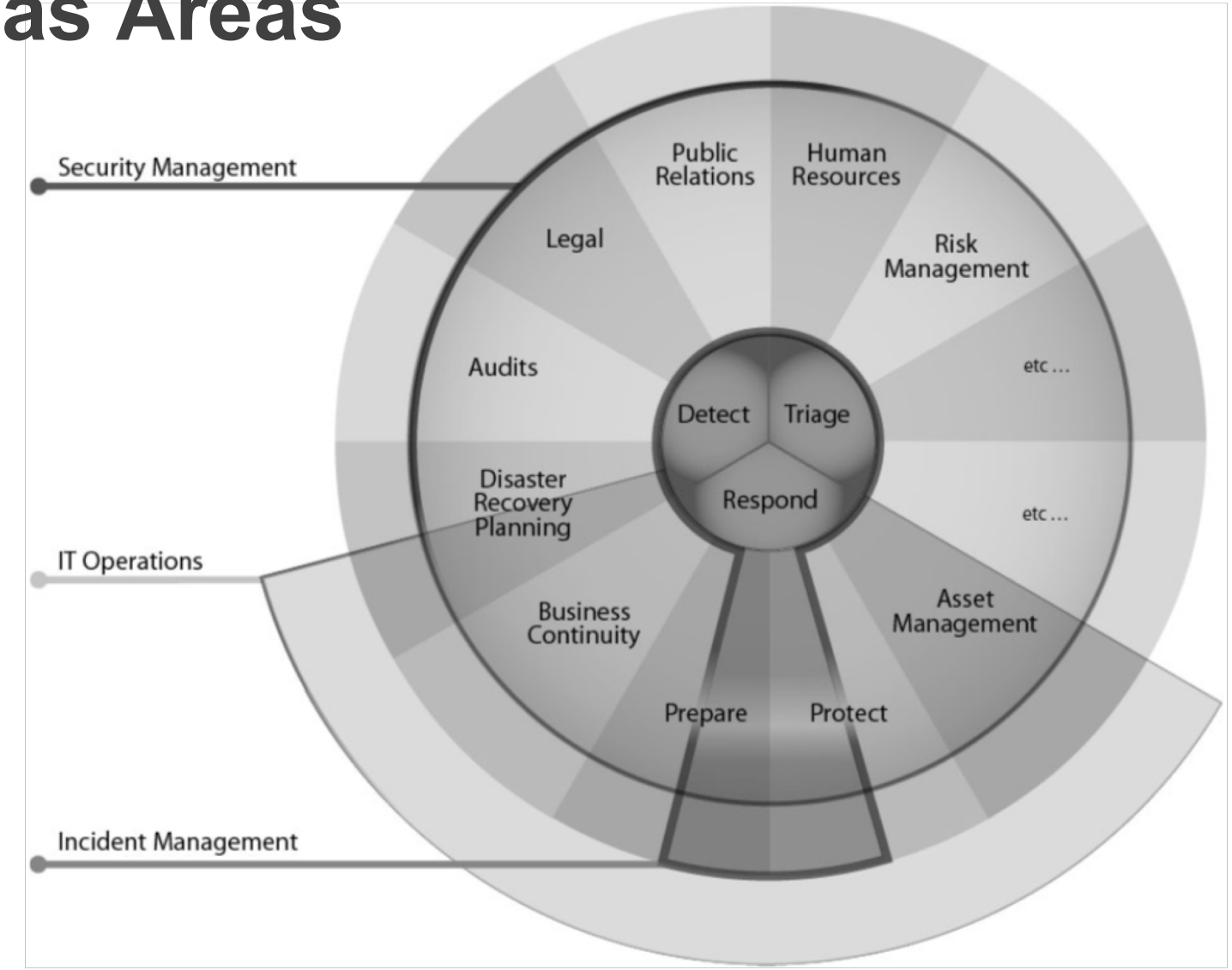
- comunica-se com todas as partes da organização e seus processos
- é imprescindível definir interfaces e pontos de contato efetivos

Operações de TI

- precisam aprimorar a detecção de eventos e possíveis incidentes de maneira integrada com o CSIRT
- manter sistemas atualizados é essencial

Gestão de segurança

- continua responsável por definir as medidas de segurança necessárias
- precisa mudar o foco de segurança perfeita para resiliência e tratamento rápido



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*****. Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Grupos de Resposta a Incidentes de Segurança

CSIRT (*Computer Security Incident Response Team*)

- acrônimo utilizado internacionalmente para designar um Grupo de Resposta a Incidentes de Segurança

> "Um CSIRT é uma organização ou grupo que presta serviços e suporte, para um público alvo específico, para prevenção, tratamento e resposta a incidentes de segurança em computadores."

Outros acrônimos: IRT, CIRC, CIRT, SERT, SIRT, CERT®

No Brasil também são usados: CTIR, ETIR

Resiliência das Organizações:
Papel dos CSIRTs na Mitigação e Recuperação

Tratamento de Incidentes é só um de vários processos essenciais

- Gestão de Risco, Segurança da Informação, Continuidade de Negócios, Segurança de Desenvolvimento, Gestão de Mudanças, de Atualizações e de Configuração

A redução do impacto de um incidente é consequência da

- agilidade de resposta
- redução no número de vítimas

O sucesso depende da confiabilidade

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O papel de um CSIRT é

- auxiliar a proteção da infraestrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas
- responder aos incidentes – retornar o ambiente ao estado de produção

O CSIRT não é um investigador

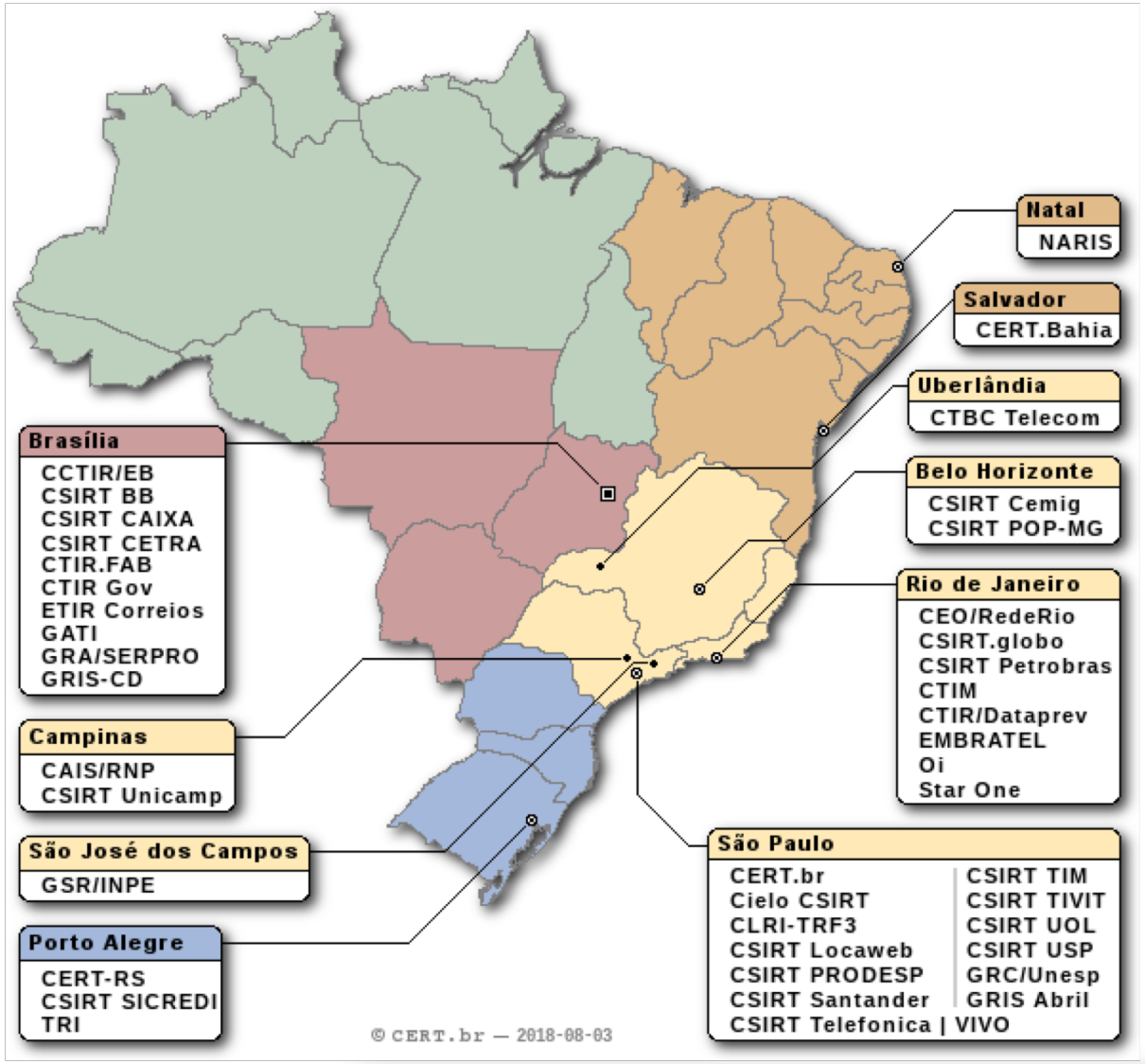
- foco é entender “o que” o que aconteceu, não “quem” originou a ação

Grupos de Tratamento de Incidentes (CSIRTs) Brasileiros:

42 times com serviços anunciados ao público

Setor	CSIRTs
Nacional – domínios .br, ASNs ou IPs alocados ao Brasil.	CERT.br
Nacional – Administração Pública Federal	CTIR Gov
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energia	CSIRT Cemig, CSIRT Petrobras
Sistema Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Provedores Operadoras Hospedagem	CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Outros	CSIRT.globo, GRIS Abril

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



Fóruns de Cooperação entre CSIRTs

Fórum Brasileiro de CSIRTs

- Evento anual para promover troca de experiências e cooperação entre CSIRTs brasileiros

Reuniões periódicas entre grupos de setores específicos

- ex: Financeiro, Governo, Telecomunicações

LAC-CSIRTs

- Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e do Caribe

Annual National CSIRTs Meeting

- Organizado pela *CERT Division of the SEI/CMU*

FIRST (Forum of Incident Response and Security Teams)

- Criação: 1990
- Membros: 442 CSIRTs, em 90 países, participantes de todos os setores;

Considerações Finais

Não há ferramenta ou política de segurança que consiga impedir uma invasão

- mas a chance de vazamento de dados reduz muito se houver gestão de incidentes efetiva

É necessário definir

- políticas com base em uma análise de risco bem feita (incluindo ataques a pessoas e "*insiders*")
- controles que promovam a segregação de dados e funções
- alertas adequados e definidos com base na análise de risco e em regras de negócio

É quase impossível aumentar a segurança de sistemas desatualizados

- sistemas personalizados (feitos sob encomenda) ou desenvolvidos internamente precisam considerar ciclo de desenvolvimento seguro
  - ter atualização contínua
  - permitir que o sistema operacional seja atualizado

Investimento em capital humano é essencial

- não há ferramenta, sistema ou algoritmo que substitua um analista bem capacitado
- esse analista, usando uma boa ferramenta, é que fará a diferença

Referências e Leituras Recomendadas

Criando um Grupo de Respostas a Incidentes de Segurança em Computadores: Um Processo para Iniciar a Implantação
https://www.cert.br/certcc/csirts/Creating-A-CSIRT-br.html

Defining Incident Management Processes for CSIRTs: A Work in Progress
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7153

NIST SP 800-61 Rev 2. *Computer Security Incident Handling Guide*
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Action List for Developing a Computer Security Incident Response Team (CSIRT)
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53102

Common Sense Guide to Mitigating Insider Threats, Sixth Edition
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

NBR ISO/IEC 27000
http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada

Information Security Policies Made Easy, Charles Cresson Wood, 13th edition
https://www.rothstein.com/product/information-security-policies-made-easy/

Obrigada

www.cert.br

cristine@cert.br @certbr

25 de abril de 2019

nic.br cgi.br

www.nic.br | www.cgi.br