nic.br cgi.br | cert.br

11º Seminário de Proteção à Privacidade e aos Dados Pessoais

18 de novembro de 2020

Evento *Online*

Gestão de Incidentes no Contexto da Proteção de Dados

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

Gestão de Incidentes na LGPD:
A palavra incidente é citada 6 vezes

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de **incidente de segurança** que possa acarretar risco ou dano relevante aos titulares.

[…]

IV - os **riscos** relacionados ao **incidente**;

[…]

§ 2º A autoridade nacional verificará a **gravidade do incidente** e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

[…]

II - medidas para reverter ou **mitigar os efeitos do incidente**.

§ 3º No juízo de **gravidade do incidente**, será avaliada eventual comprovação de que foram adotadas **medidas técnicas adequadas** que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

[…] Art. 50. […]

g) conte com **planos de resposta a incidentes** e remediação;

[…]

Antes de Falar em Gestão de Incidentes: **Análise de Risco é Pré-requisito**

Riscos:
- indisponibilidade de serviços
- perda de privacidade
- furto ou destruição de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Ativos
(Sistemas e Dados)

Ameaças

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

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

Opções para lidar com o risco:

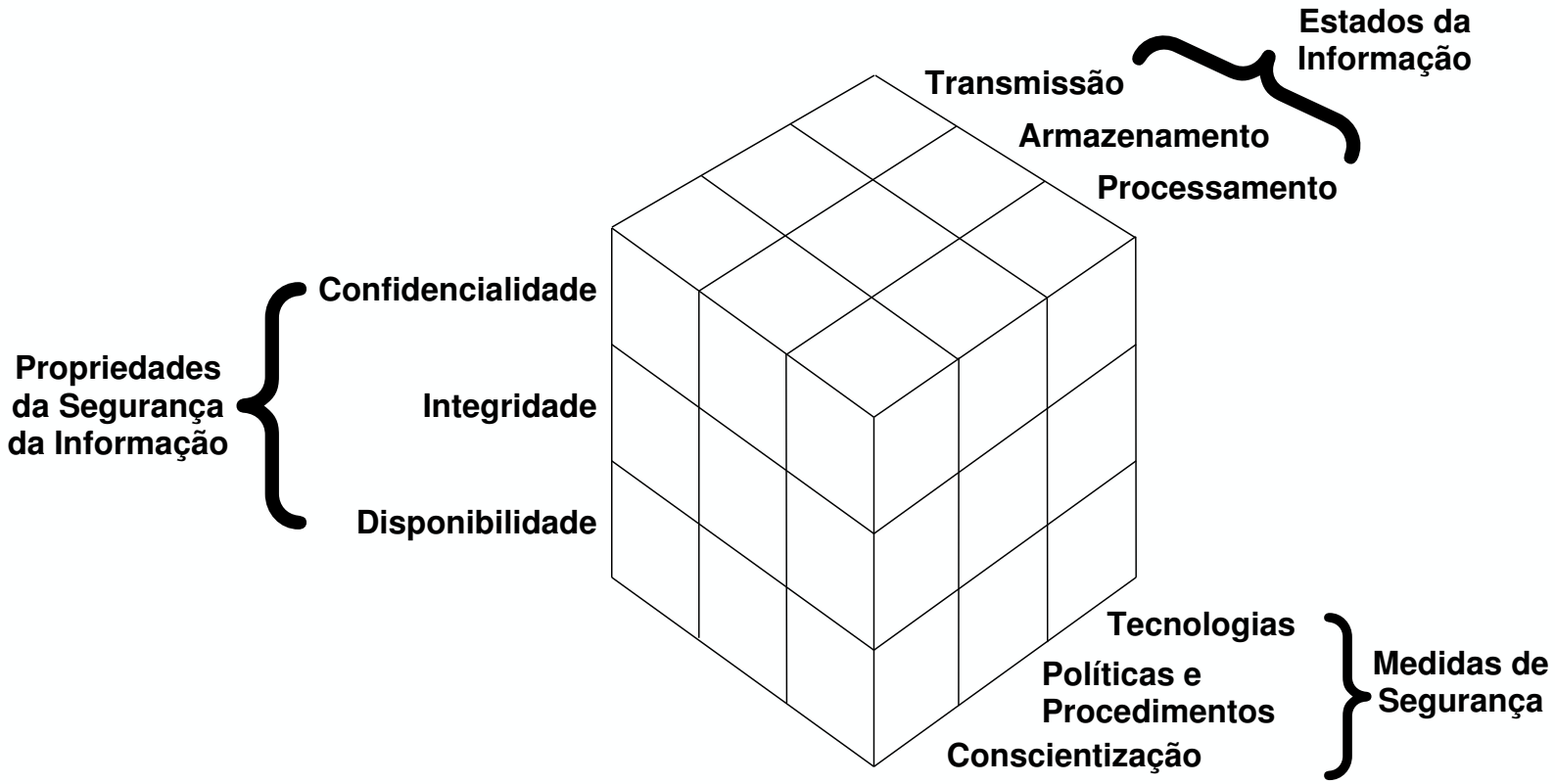
Aceitar

Transferir
- ex: seguro

Eliminar
- remover um dos vértices

Mitigar (gestão de risco)
- única real opção

Segurança da Informação:
É um Processo Complexo



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

Considerações:

Os dados estão em diversos locais e a segurança depende de múltiplos fatores

Não é possível "garantir" segurança

- fator humano (*insiders*)
- novas vulnerabilidades (*0-day vulnerabilities*)
- sistemas legados (*n-day/forever-day vulnerabilities*)

É possível:

- mitigar os riscos e reduzir a probabilidade de vazamentos e acessos indevidos
- **ter gestão de incidentes: detectar precocemente e reduzir os danos**

Incidentes Observados pelo CERT.br:
Causas Mais Comuns de Invasões e Vazamentos

Ataques mais reportados e mais observadores em sensores:

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
  - *e-mails* e serviços em nuvem
  - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
  - falta de aplicação de correções

Fontes:
Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

- todos os *patches* fossem aplicados
- todos os serviços tivessem 2FA/MFA

Apelo para DPOs e Gestores

- Priorizem a adoção de MFA (*Multi-Factor Authentication*)
  - ex: aplicativo autenticador ou *token* (ex: Yubikey)
- Motivos usuais para não adoção
  - diminui a conveniência
  - pode incorrer em custos
  - requer treinamento dos técnicos e usuários
  - medo de perder acesso aos serviços

Ainda temos os 20% restantes:
Mesmo os Sistemas Mais Seguros São Invadidos

- 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 certificados falsos do Google, usados 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

Organizações Precisam Alcançar Resiliência

Um sistema 100% seguro é impossível de atingir: incidentes ocorrerão

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

***Checklist*:**

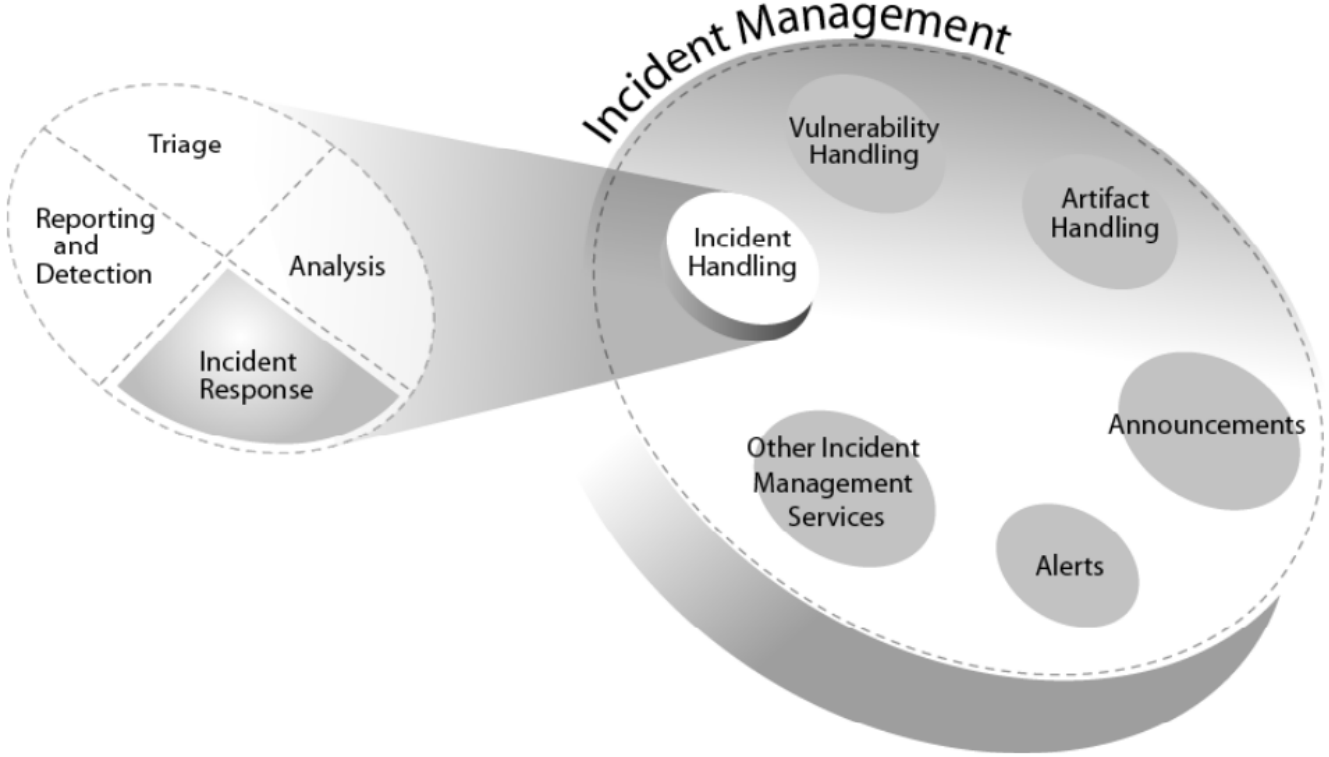
- **Identificar o que é crítico** e precisa ser mais protegido (Análise de Risco)
- **Definir políticas** (de uso aceitável, acesso, segurança, etc)
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- **Implantar medidas de segurança** que implementem as políticas de segurança
  - ex: 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)**

Gestão de Incidentes: **Definições**

Gestão de Incidentes – políticas e estratégias
- gestão fim a fim de eventos e incidentes
- envolve toda a organização

Tratamento de Incidentes – processos
- identificar, prevenir, mitigar e responder

Resposta a Incidentes – ações
- resolver ou mitigar incidentes
- disseminar informações
- 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

Gestão de Incidentes: **Processos**

Preparação da organização

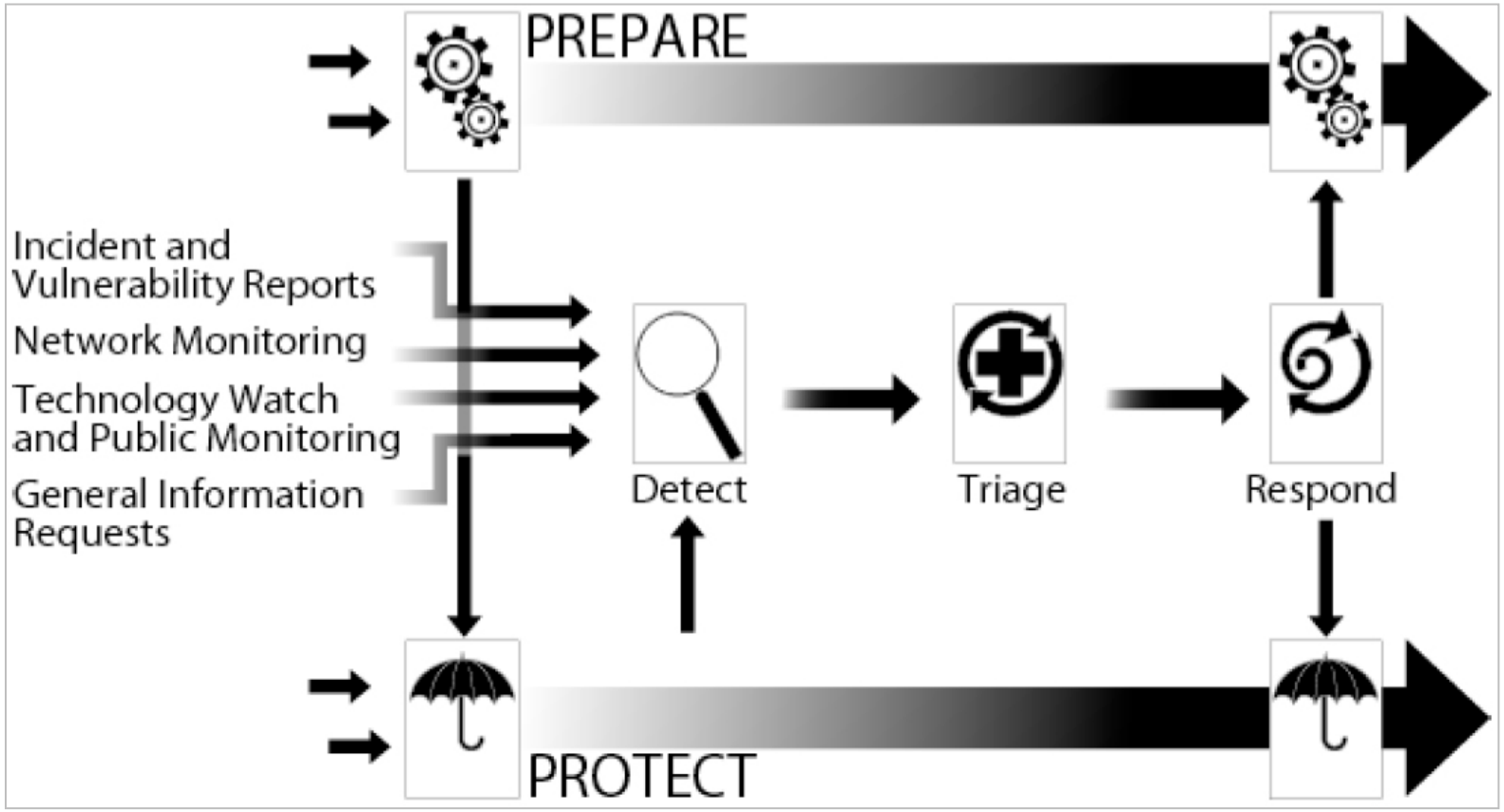
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT

Proteção da infraestrutura

- processo contínuo de implementação de medidas de segurança

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

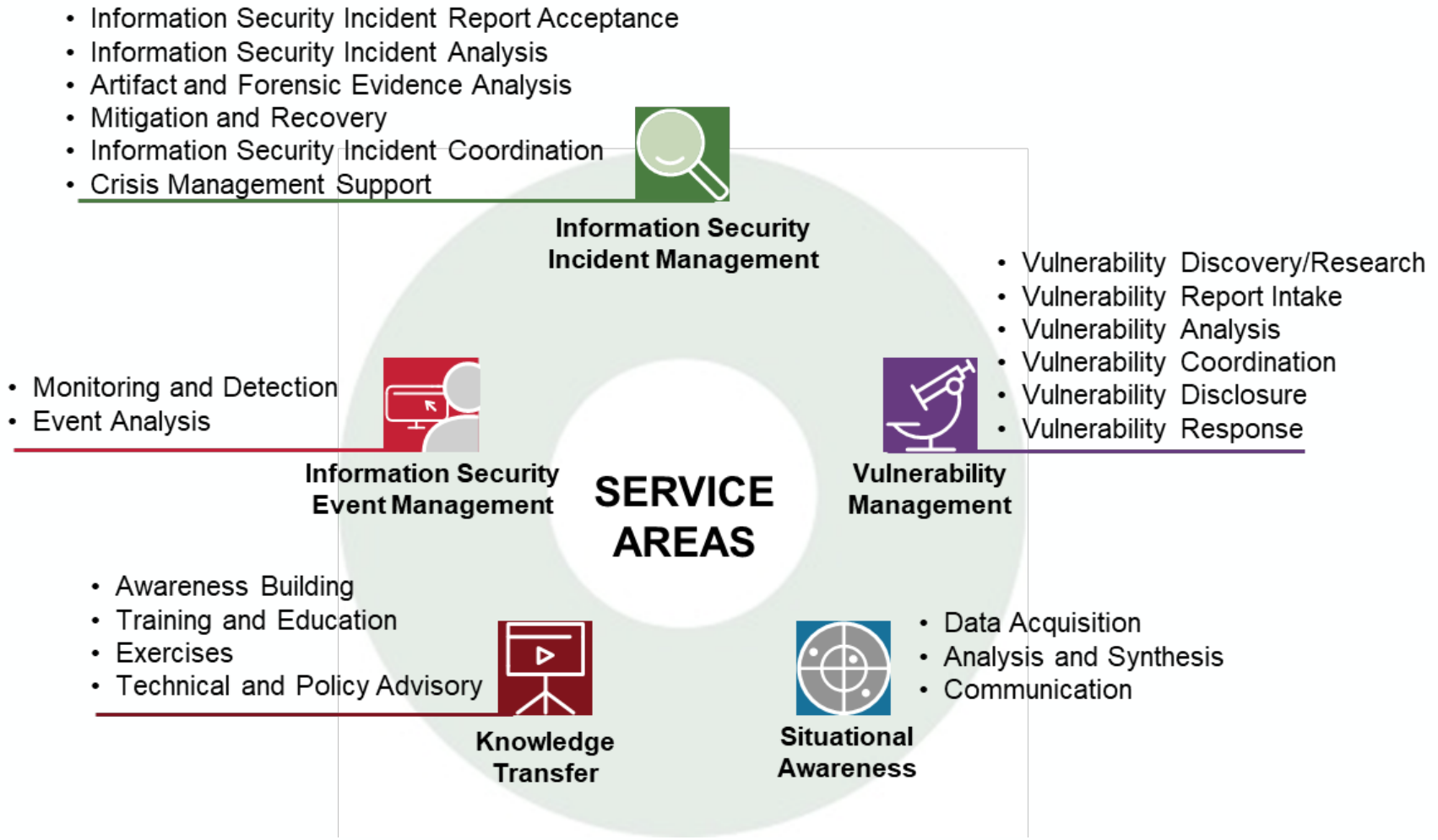
Gestão de Incidentes: **Serviços e Funções**

"The Computer Security Incident Response Team (CSIRT) Services Framework is

- *a high-level document*
- *describing in a structured way*
- *a collection of cyber security services and associated functions*

that Computer Security Incident Response Teams and other teams providing incident management related services may provide."

"The services described are those potential services a CSIRT could provide. No CSIRT is expected to provide all described services."



***Computer Security Incident Response Team (CSIRT) Services Framework*:**
https://www.first.org/standards/frameworks/csirts/

Gestão de Incidentes não está Isolada:
Pode ser Encontrada em todos os *Frameworks*

"The Framework is

- *voluntary guidance,*
- *based on existing standards, guidelines, and practices*
- *for organizations to better manage and reduce cybersecurity risk.*

In addition to helping organizations manage and reduce risks, it was designed to

- *foster risk and cybersecurity management communications*
- *amongst both internal and external organizational stakeholders."*

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Incident Management

Original em Inglês e tradução para o Português disponíveis em:
https://www.nist.gov/cyberframework/framework

Referências Adicionais

cert.br nic.br cgi.br

Atividades de Fomento do CERT.br:
Criação de Uma Comunidade Atuante

Premissa: Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes.

Foco

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos

Lista de CSIRTs Brasileiros

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

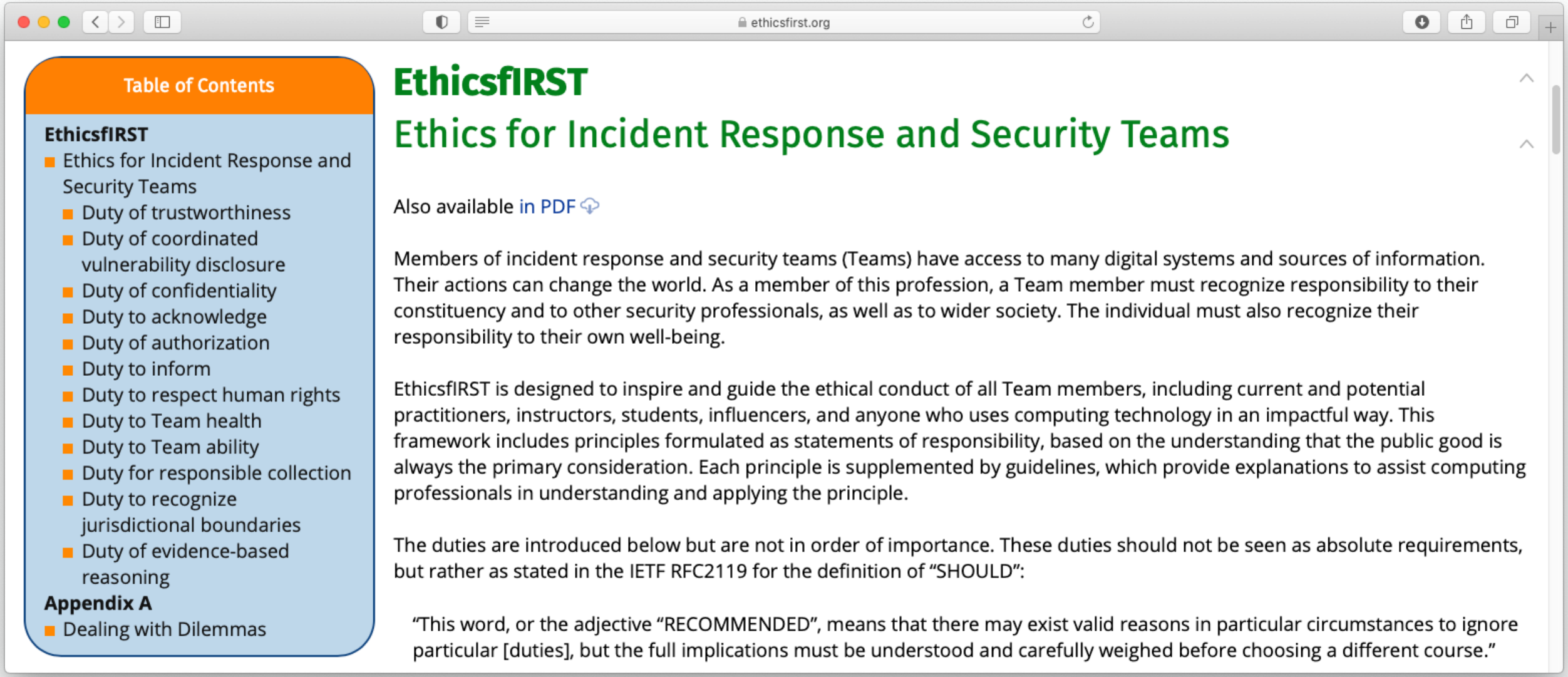
Cursos de Gestão de Incidentes

Ministra os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2004:

- https://cert.br/cursos/

SEI Partner Network

EthicsfIRST.org:
Código de Ética da Comunidade Global de CSIRTs



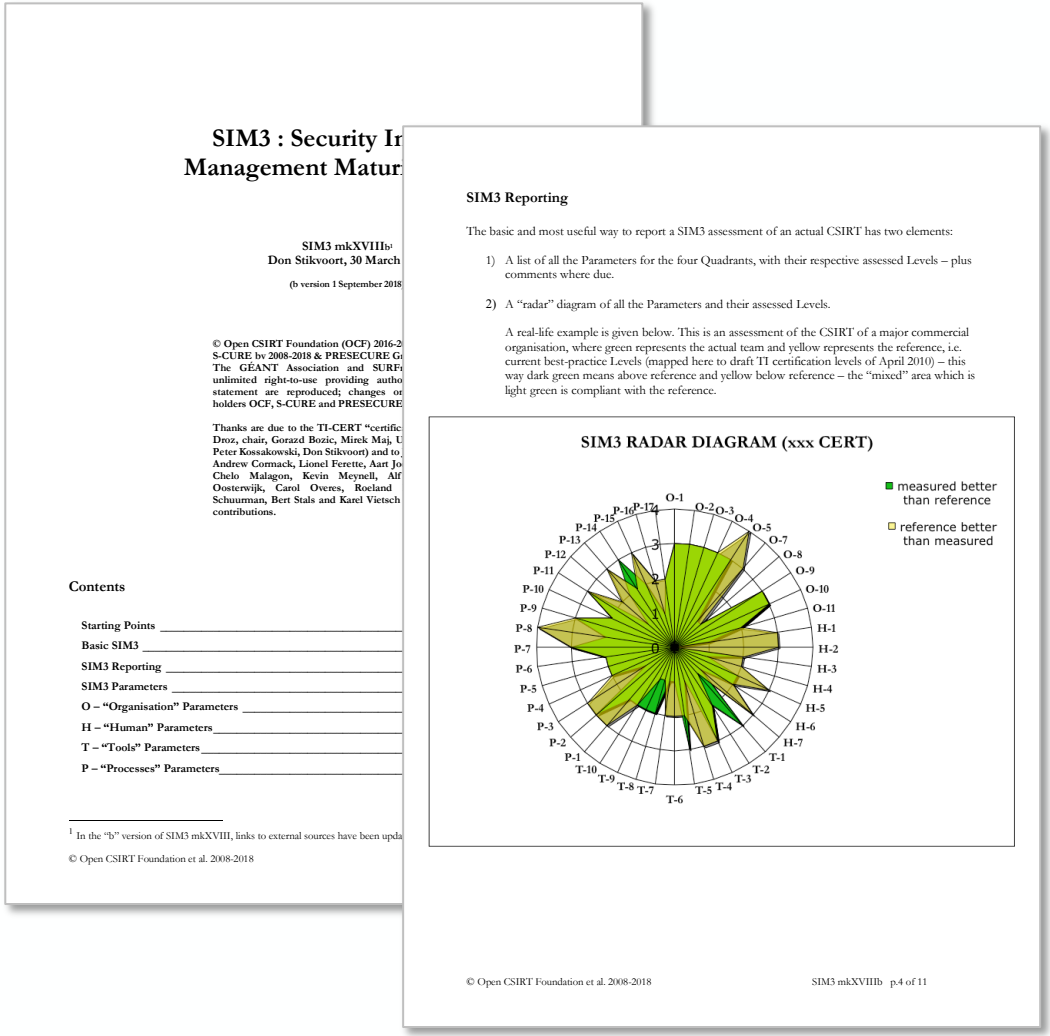
Avaliação de Maturidade:
SIM3 – *Security Incident Management Maturity Model*

Quatro pilares
- Prevenção
- Detecção
- Resolução
- Controle de qualidade e *feedback*

Quatro quadrantes
- O – *Organisation* (11 parâmetros)
- H – *Human* (7 parâmetros)
- T – *Tools* (10 parâmetros)
- P – *Processes* (17 parâmetros)

Quem usa
- *TF-CSIRT Trusted Introducer*
- ENISA, requerimento para CERTs Nacionais (NIS Directive)
- *Nippon CSIRT Association*
- FIRST: será adotado no processo de filiação

https://opencsirt.org/maturity/sim3/
https://thegfce.org/initiatives/csirt-maturity-initiative/


SIM3 : Security In
Management Matur

SIM3 mkXVIIIb[1]
Don Stikvoort, 30 March

(b version 1 September 2018

© Open CSIRT Foundation (OCF) 2016-2
S-CURE bv 2008-2018 & PRESECURE G
The GÉANT Association and SURF
unlimited right-to-use providing autho
statement are reproduced; changes or
holders OCF, S-CURE and PRESECURE

Thanks are due to the TI-CERT "certific
Droz, chair, Gorazd Bozic, Mirek Maj, U
Peter Kossakowski, Don Stikvoort) and to
Andrew Cormack, Lionel Ferette, Aart Jo
Chelo Malagon, Kevin Meynell, Alf
Oosterwijk, Carol Overes, Roeland
Schuurman, Bert Stals and Karel Vietsch
contributions.

Contents

Starting Points
Basic SIM3
SIM3 Reporting
SIM3 Parameters
O – "Organisation" Parameters
H – "Human" Parameters
T – "Tools" Parameters
P – "Processes" Parameters

[1] In the "b" version of SIM3 mkXVIII, links to external sources have been upda

© Open CSIRT Foundation et al. 2008-2018

SIM3 Reporting

The basic and most useful way to report a SIM3 assessment of an actual CSIRT has two elements:

1) A list of all the Parameters for the four Quadrants, with their respective assessed Levels – plus comments where due.
2) A "radar" diagram of all the Parameters and their assessed Levels.

A real-life example is given below. This is an assessment of the CSIRT of a major commercial organisation, where green represents the actual team and yellow represents the reference, i.e. current best-practice Levels (mapped here to draft TI certification levels of April 2010) – this way dark green means above reference and yellow below reference – the "mixed" area which is light green is compliant with the reference.

SIM3 RADAR DIAGRAM (xxx CERT)

measured better than reference
reference better than measured

© Open CSIRT Foundation et al. 2008-2018 SIM3 mkXVIIIb p.4 of 11

SIM3:
Online Tool

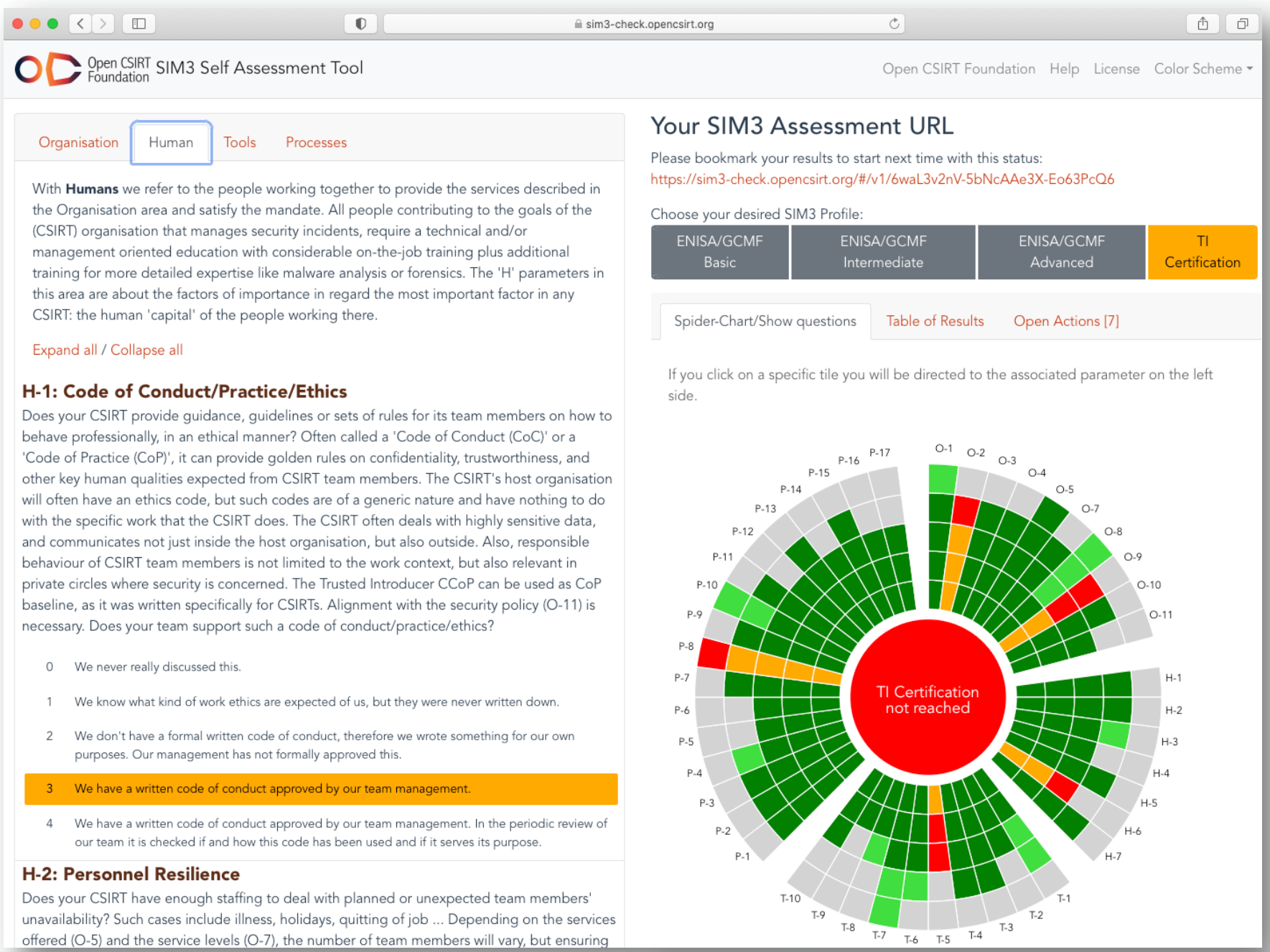
Auto avaliação em forma de perguntas

Possui 4 perfis

- *Trusted Introducer TI Certification*
- ENISA
  - *Basic*
  - *Intermediate*
  - *Advanced*

Será incluído um perfil para o FIRST, quando for adotado para filiação

https://sim3-check.opencsirt.org/



Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br