nic.br cgi.br | cert.br

I Workshop de Tratamento de Incidentes Cibernéticos para ETIRs da Defesa

Comando de Defesa Cibernética (ComDCiber)

07 de novembro de 2023

Brasília, DF

Boas Práticas para Gestão de Incidentes Cibernéticos

Cristine Hoepers, Dra.
Gerente, CERT.br/NIC.br
cristine@cert.br

Klaus Steding-Jessen, Dr.
Gerente Técnico, CERT.br/NIC.br
jessen@cert.br

TLP conforme padrão do FIRST
https://cert.br/tlp/

Slides ficarão *online* em
https://cert.br/docs/palestras/

cert.br nic.br cgi.br

TLP:CLEAR

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST: Membro pleno desde 2002 | **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020

APWG: *Research partner* desde 2004 | **SEI/CMU:** Cursos autorizados desde 2003

***Honeynet Project*:** Mantém o capítulo do Brasil desde 2003

https://cert.br/sobre/ | https://cert.br/sobre/filiacoes/ | https://cert.br/about/rfc2350/

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Foco do CERT.br nestes 26 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum time ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Times** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

Comunidade Internacional

- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

Incidentes não Respeitam Fronteiras: **Cooperação entre CSIRTs no Mundo**

Há diversas comunidades

Algumas mais efetivas que outras

Próximos *slides* contém reflexões com base no conteúdo do seguinte treinamento do FIRST:

- Incident Handling for Policy Makers

  "Participants will learn how incident response on a global scale functions and what the preconditions for establishing a successful CSIRT community are. Rather than presenting simple recipes the training focuses on concepts which are worked out by analysing real world incidents."

  https://www.first.org/education/trainings
  https://www.first.org/education/incident_handling_for_policy_makers/Incident_Response_for_Policymakers_v1.2.3.pptx.zip

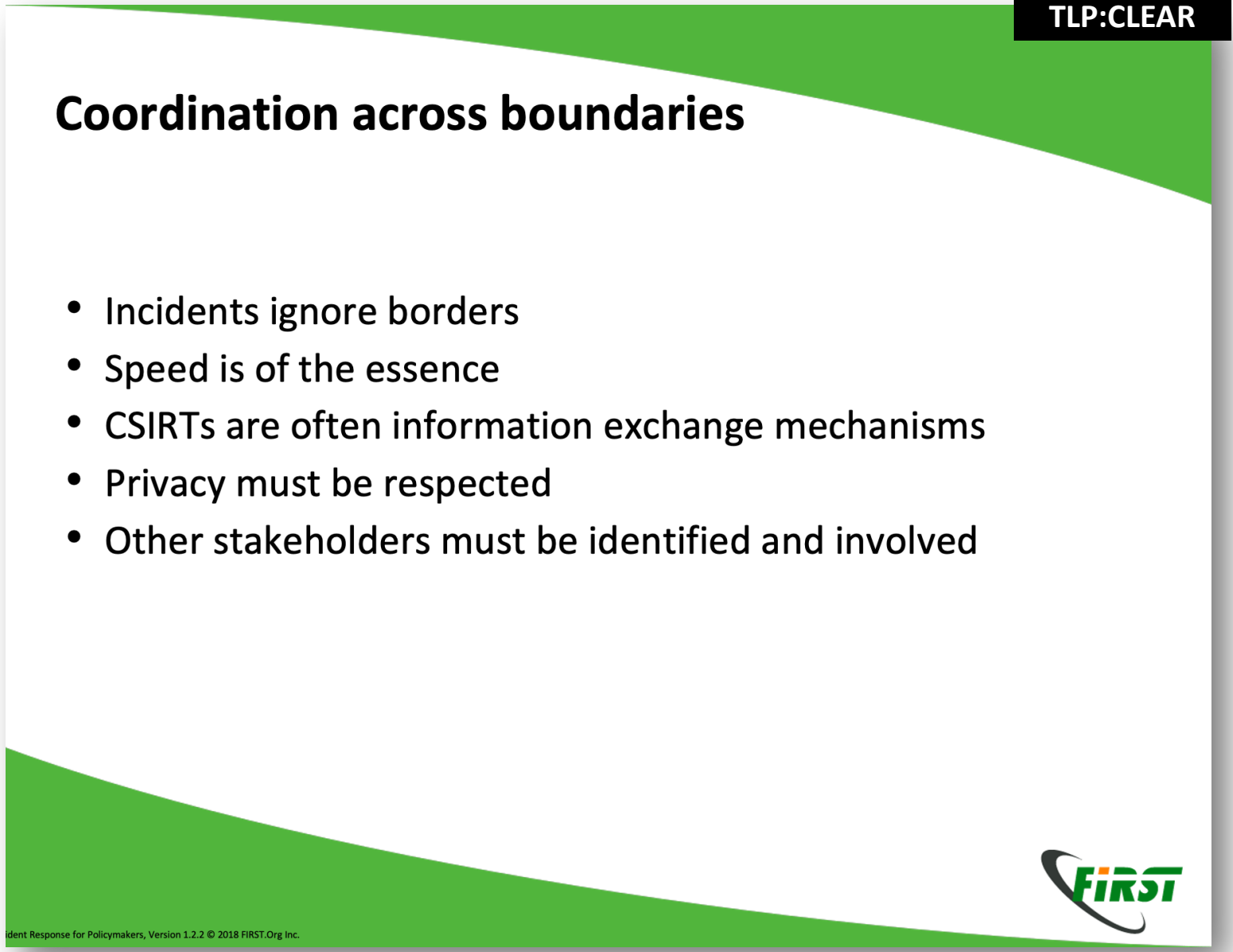
CSIRTs Efetivos Cooperam Diretamente

Objetivo maior é proteger

- Redes
- Informações
- Cidadãos

Independente de

- Normas locais
- Redes em que participam
- Setores a que pertencem



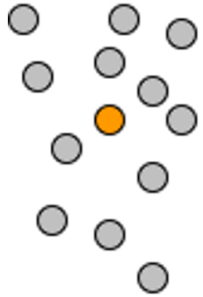
Existem Diferentes formas de Governança

CSIRTs se coordenam em redes

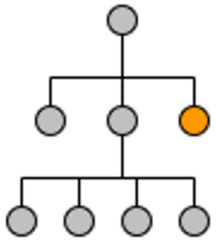
- um CSIRT pode participar de múltiplas redes

Forms of governance

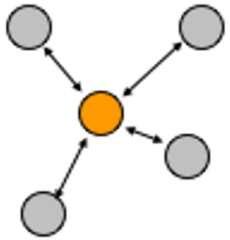
Market



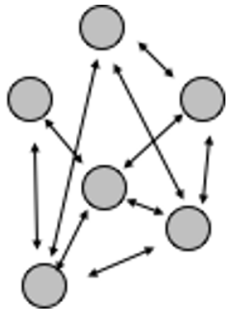
Hierarchy



Collaboration



Network



Network governance

*Governance [is achieved] through relatively **stable** cooperative relationships between three or more legally autonomous organisations **based on horizontal**, rather than hierarchical coordination, recognizing one or more network or collective goals*

The late Elinor Ostrom receives the 2009 economic sciences Nobel price for her ground-breaking work: “Governing the Commons”.

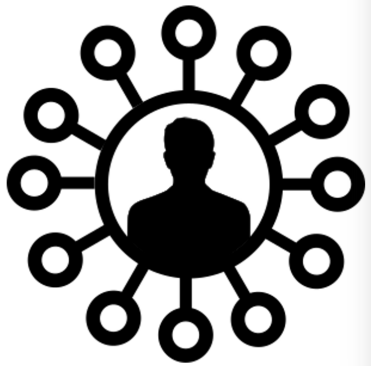
Source: https://commons.wikimedia.org/wiki/File:Nobel_Prize_2009-Press_Conference_KVA-31.jpg

CSIRTs Dependem de Redes de Confiança

Também precisam

- Agilidade de Comunicação
- Informalidade
- *Expertise*

In a network different organizations work together, Even competitors!



CSIRTs as networks

- CSIRTs collaborate across the world in networks
  - APCERT
  - FIRST
  - OIC-CERT
  - TF-CSIRT
- CSIRTs also cooperate with other organizations that may not always be called CSIRTs. Organizations have the responsibility to respond to incidents, even when they do not staff for it proactively.
- This works well if the preconditions are satisfied.

Confiança Depende de Fatores Subjetivos

É construída ao longo do tempo

- Reuniões periódicas
- Cooperação contínua
- Projetos em conjunto

Effective network collaboration requires **trust** and a **common goal**.

If either is missing collaboration is not possible.

How do you build Trust?

- Ensure there is a good understanding of **roles and responsibilities**
- Have strong Points of Contact that have **functional networks**
- Build on a **history of working together** and meeting each other's expectations
- Use of **good standards** and **similar terminology**
- **NDAs and contracts** play a lesser role

TLP:CLEAR

Padrões para Operação de CSIRTs Efetivos

cert.br nic.br cgi.br

CSIRT - *Computer Security Incident Response Team*

- Um **Time de Resposta a Incidentes de Segurança em Computadores** (CSIRT) é uma unidade organizacional (que pode ser virtual) ou uma estrutura (capability) que **fornece serviços e apoio** a um **público-alvo definido** para **prevenir, detectar, tratar e responder a incidentes de segurança** em computadores, de acordo com a sua missão.

Fonte: *FIRST CSIRT Services Framework*
https://www.first.org/standards/frameworks/csirts/

Questões chave para o sucesso de um CSIRT

- Criar um ambiente favorável à notificação de incidentes
  - sem caráter punitivo
  - não pode ser confundido com auditoria
- Criar relações de confiança
- Ter uma rede de contatos
  - especialistas e outros CSIRTs

CSIRTs
Evolução e Desafios

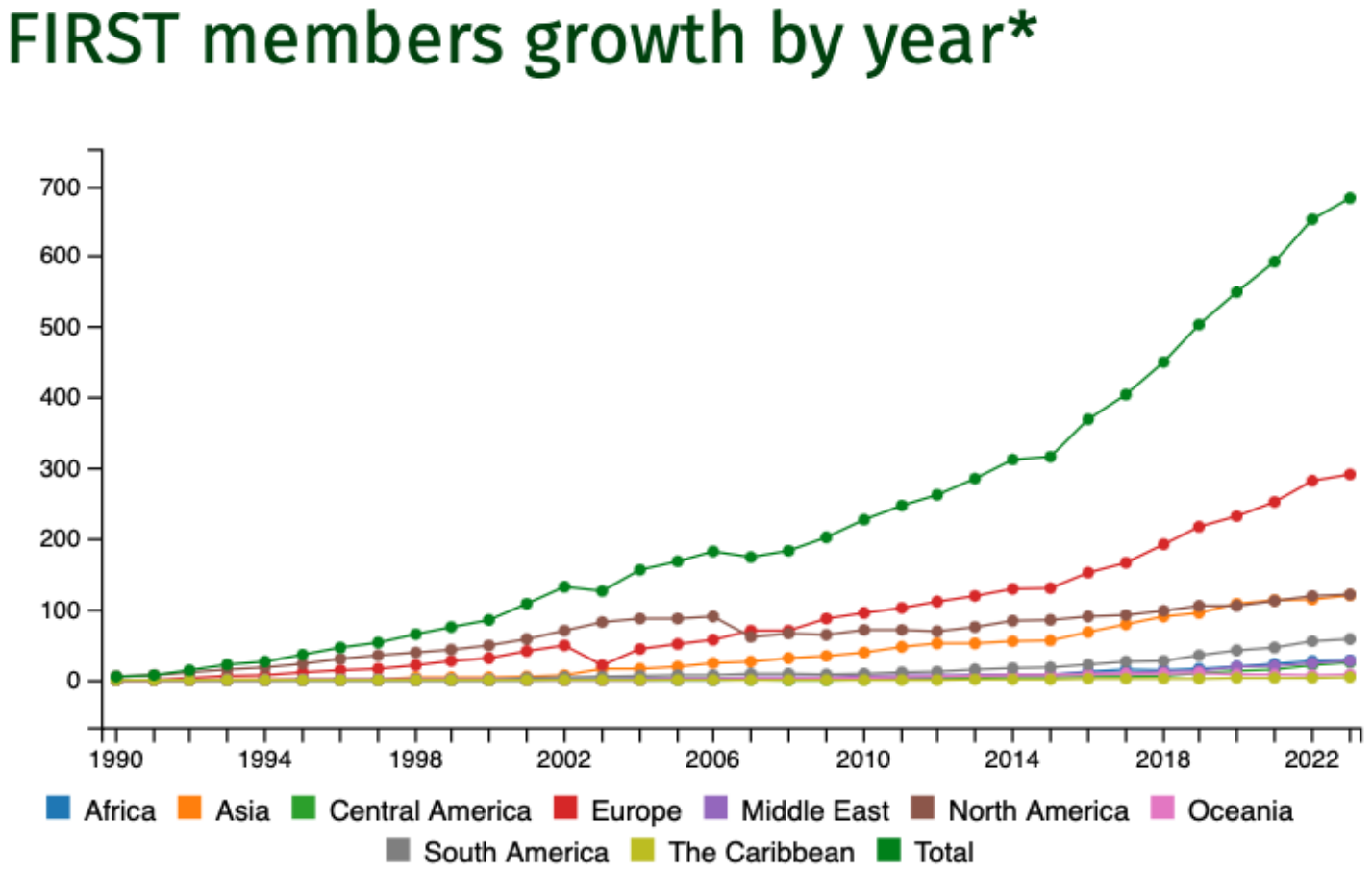
Número crescente

- Diversos países
- Diversos setores
- Variados níveis de maturidade

Confiança (*trust*) é pré-requisito para cooperação

Desafios

- Como identificar serviços necessários?
- Como quantificar a maturidade e a qualidade dos serviços?
- Como respeitar as expectativas de confidencialidade?
- Como identificar habilidades e conhecimentos necessários aos profissionais dessa área?



(*) The statistic measurement method and regional breakdown changed in 2007.

Fonte: *FIRST History*, *link* visitado em 06/11/2023
https://www.first.org/about/history

Padrões de Serviços e Maturidade **Essenciais para um CSIRT Efetivo**

- Sob Coordenação do FIRST
  - **CSIRT *Services Framework***
  - **EthicsfIRST (Ethics for Incident Response and Security Teams)**
  - **TLP (*Traffic Light Protocol*)**
  - PSIRT *Services Framework*
  - CVSS (*Common Vulnerability Scoring System*)
  - IEP (*Information Exchange Policy*)
  - EPSS (*Exploit Prediction Scoring System*)
- Sob coordenação da *Open* CSIRT *Foundation*
  - **SIM3 (*Security Incident Management Maturity Model*)**

Organizações envolvidas no desenvolvimento destes padrões

FIRST (*Forum of Incident Response and Security Teams*)

Open CSIRT *Foundation*

TF-CSIRT

ENISA (*European Union Agency for Cybersecurity*)

GFCE (*Global Forum on Cyber Expertise*)

CSIRT *Services Framework*

Descrição em alto nível dos possíveis serviços que possam ser oferecidos

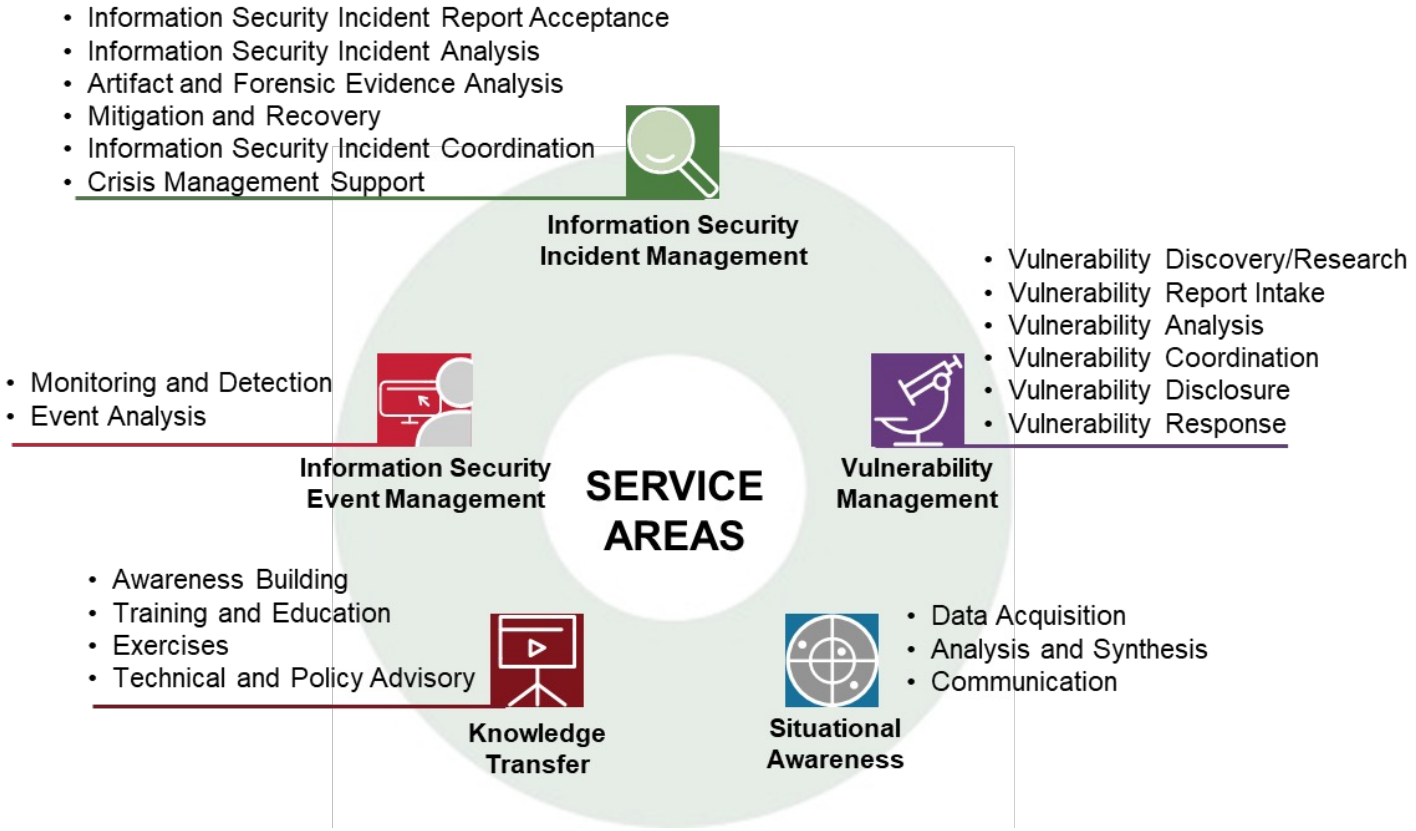
- por um CSIRT
- por times com serviços relacionados com gestão de incidentes

Objetivo de auxiliar times a

- identificar e definir quais serviços são essenciais para seu contexto
- identificar termos e definições usados pela comunidade

CSIRT Roles and Competences

- papéis e competências para as funções, com base no padrão NICE do NIST



https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
https://www.first.org/standards/frameworks/csirts/csirt_roles_competences

Team Types Within the Context of Services Frameworks
Serviços Esperados para CSIRTs

Service Area	SOC	CSIRT	PSIRT	ISAC
Information Security Event Management				
Monitoring and Detection	MUST	-	-	-
Event Analysis	MUST	-	-	-
Information Security Incident Management				
Information Security Incident Report Acceptance	-	MUST	-	-
Information Security Incident Analysis	-	MUST	-	-
Artifact and Forensic Evidence Analysis	-	-	-	-
Mitigation and Recovery	-	MUST	-	-
Information Security Incident Coordination	-	MUST	-	-
Crisis Management Support	-	-	-	-

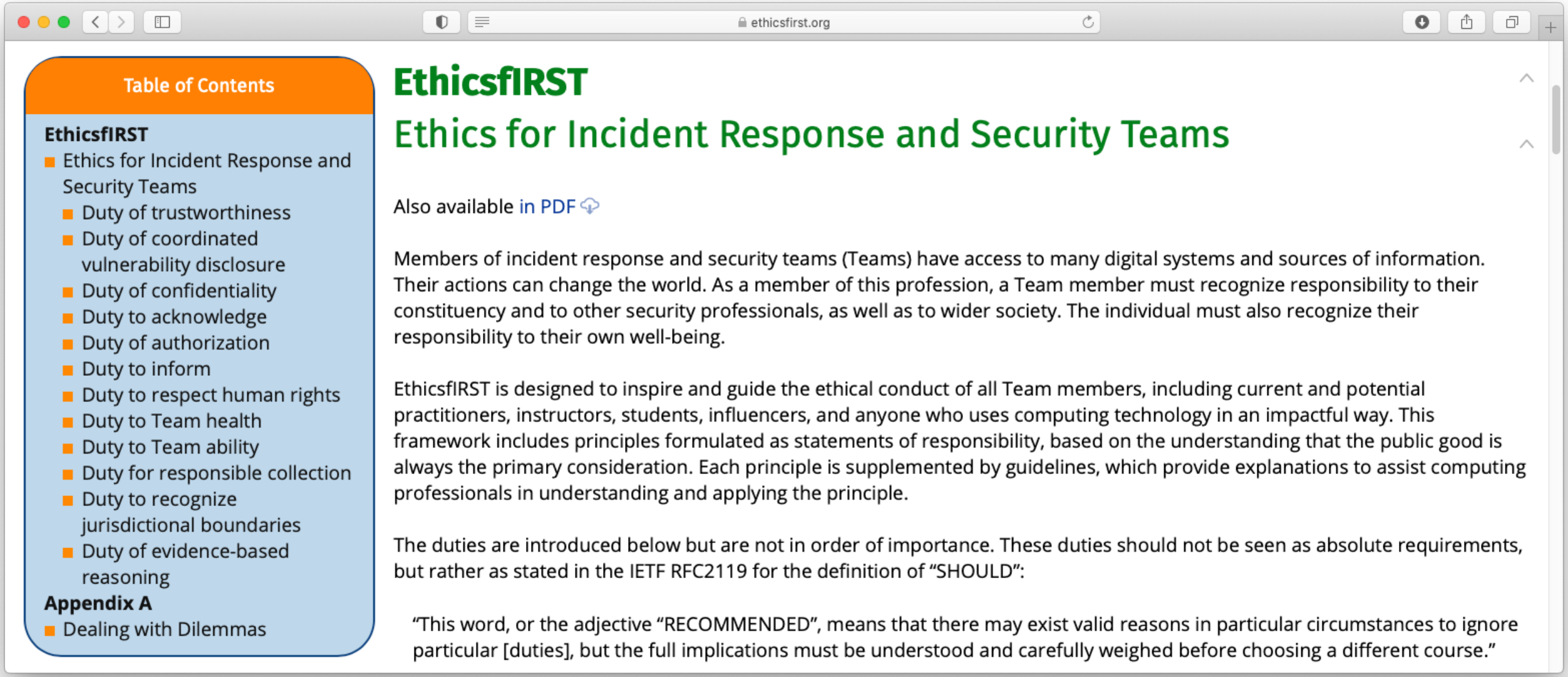
https://www.first.org/standards/frameworks/csirts/team-type

Team Types Within the Context of Services Frameworks
Serviços Esperados para CSIRTs (cont.)

Service Area	SOC	CSIRT	PSIRT	ISAC
Vulnerability Management				
Vulnerability Discovery/Research	-	-	-	-
Vulnerability Report Intake	-	-	MUST	-
Vulnerability Analysis	-	-	MUST	-
Vulnerability Coordination	-	-	MUST	-
Vulnerability Disclosure	-	-	MUST	-
Vulnerability Response	-	-	MUST	-
Situational Awareness				
Data Acquisition	-	-	-	MUST
Analysis and Synthesis	-	-	-	MUST
Communication	-	-	-	MUST

TLP:CLEAR

EthicsfIRST.org
Código de Ética da Comunidade Global de CSIRTs



Traffic Light Protocol (TLP):
Troca e Compartilhamento de Dados e Informações

O que é?
– um conjunto de **marcações**
– 4 cores para indicar os **limites de compartilhamento**

Por que?
– facilitar a adoção e a colaboração mais frequente
– aumentar a legibilidade
– facilitar **compartilhamento entre pessoas**

Onde usar?
– documentos, *e-mails*, *slides*, notificações
– plataformas de CTI, como MISP
– qualquer outro lugar (ex: Conferências)

https://cert.br/tlp/

TLP:CLEAR

Traffic Light Protocol (TLP) Versão 2.0:
Tradução Oficial - Português Brasileiro

Tradução

CERT.br/NIC.br

- Cristine Hoepers

Revisão

CAIS/RNP

- Edilson Lima
- Emilio Nakamura

CSIRT PETROBRAS

- Marcos Vinicio Rabello da Silva
- Kildane de Souza Castro

CERT.br/NIC.br

- Klaus Steding-Jessen
- Miriam von Zuben

https://www.first.org/tlp/
https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf

TLP:CLEAR

SIM3 – *Security Incident Management Maturity Model*

Quatro pilares

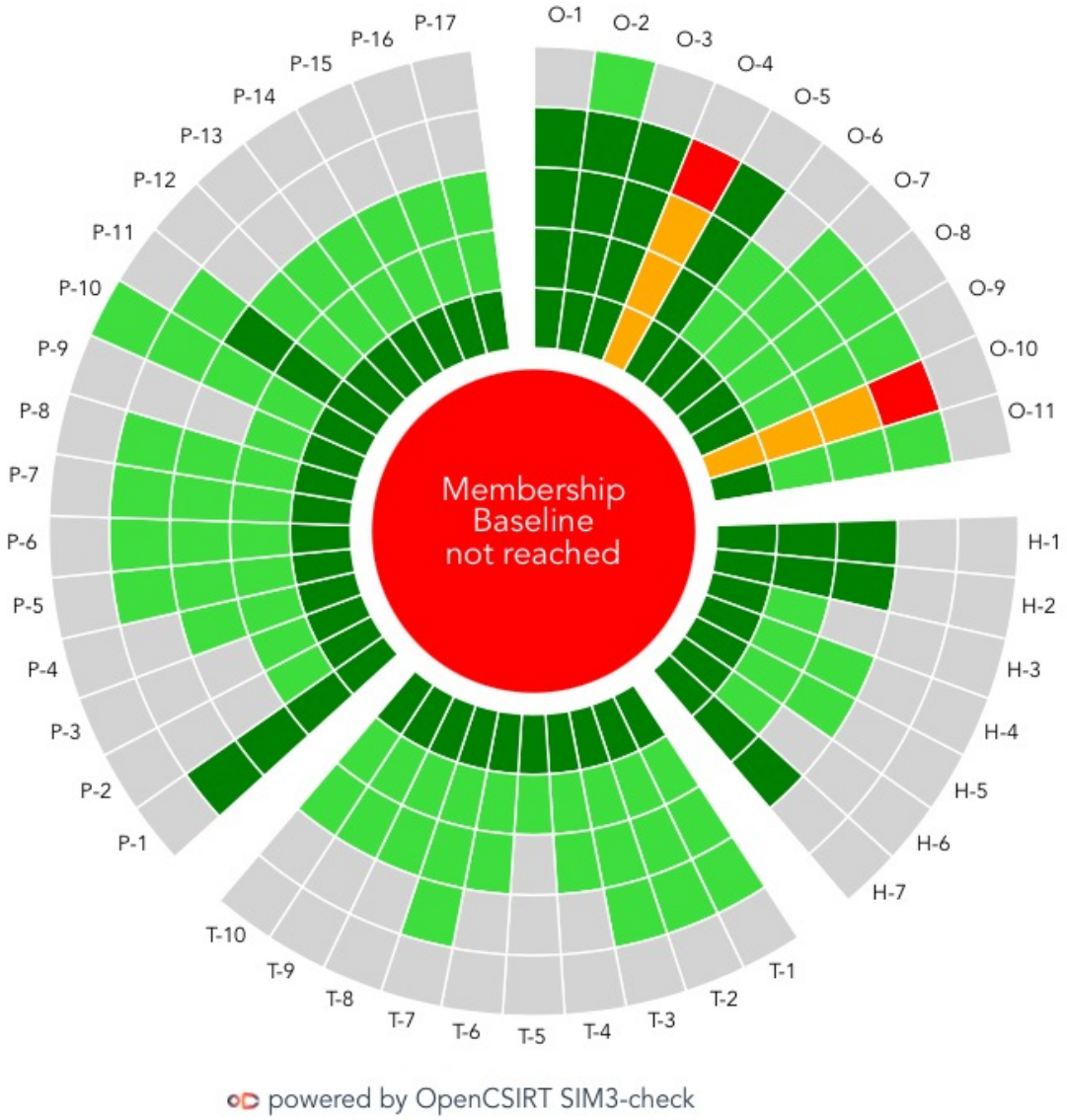
- Prevenção
- Detecção
- Resolução
- Controle de qualidade e *feedback*

Quatro quadrantes

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

Quem usa

- TF-CSIRT Trusted Introducer
- FIRST
- ENISA, requerimento para CERTs Nacionais (NIS Directive)
- Nippon CSIRT Association



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

Auto avaliação
SIM3 *Online Tool*

Em forma de perguntas

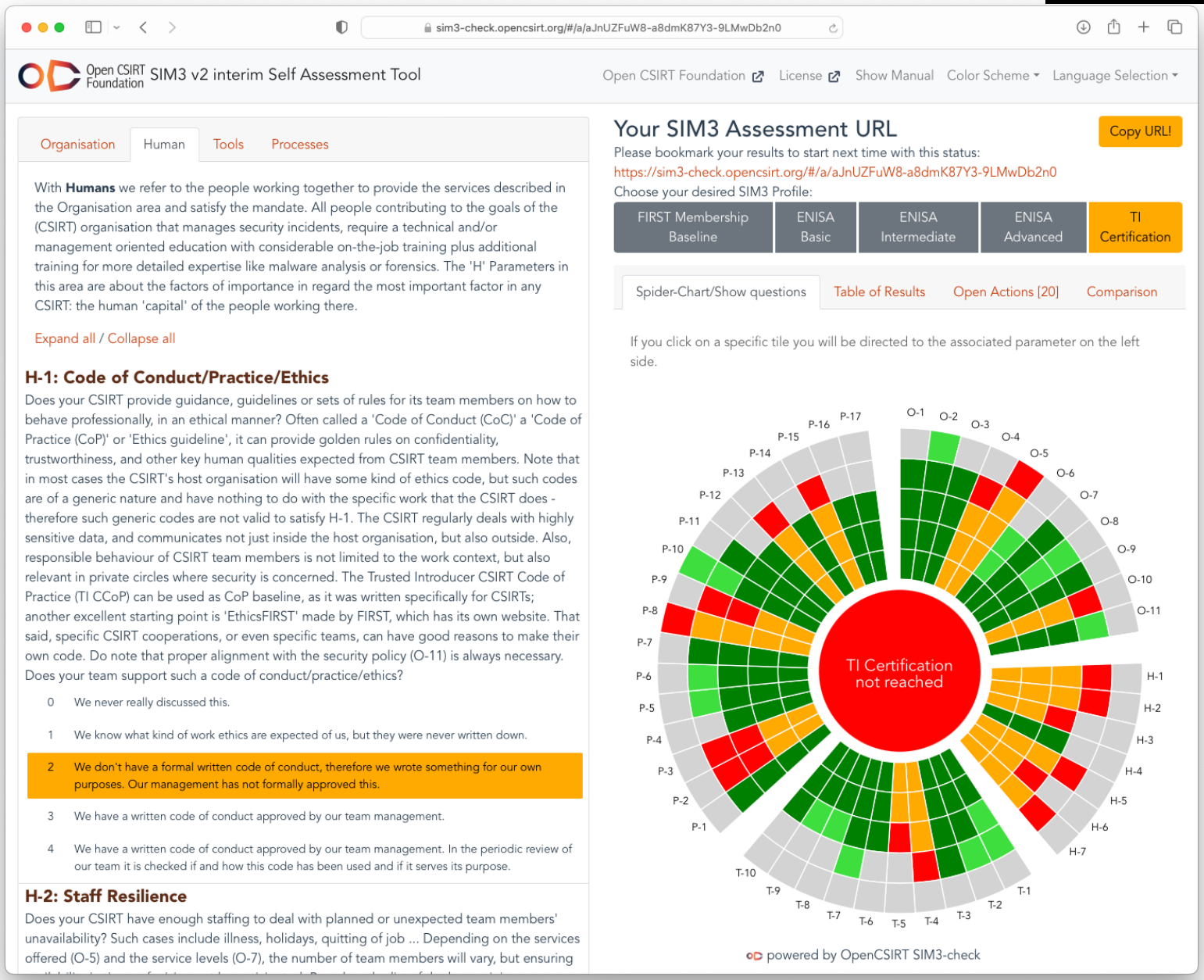
Possui 4 perfis

- FIRST Membership
- ENISA
  - *Basic*
  - *Intermediate*
  - *Advanced*
- *Trusted Introducer Certification*

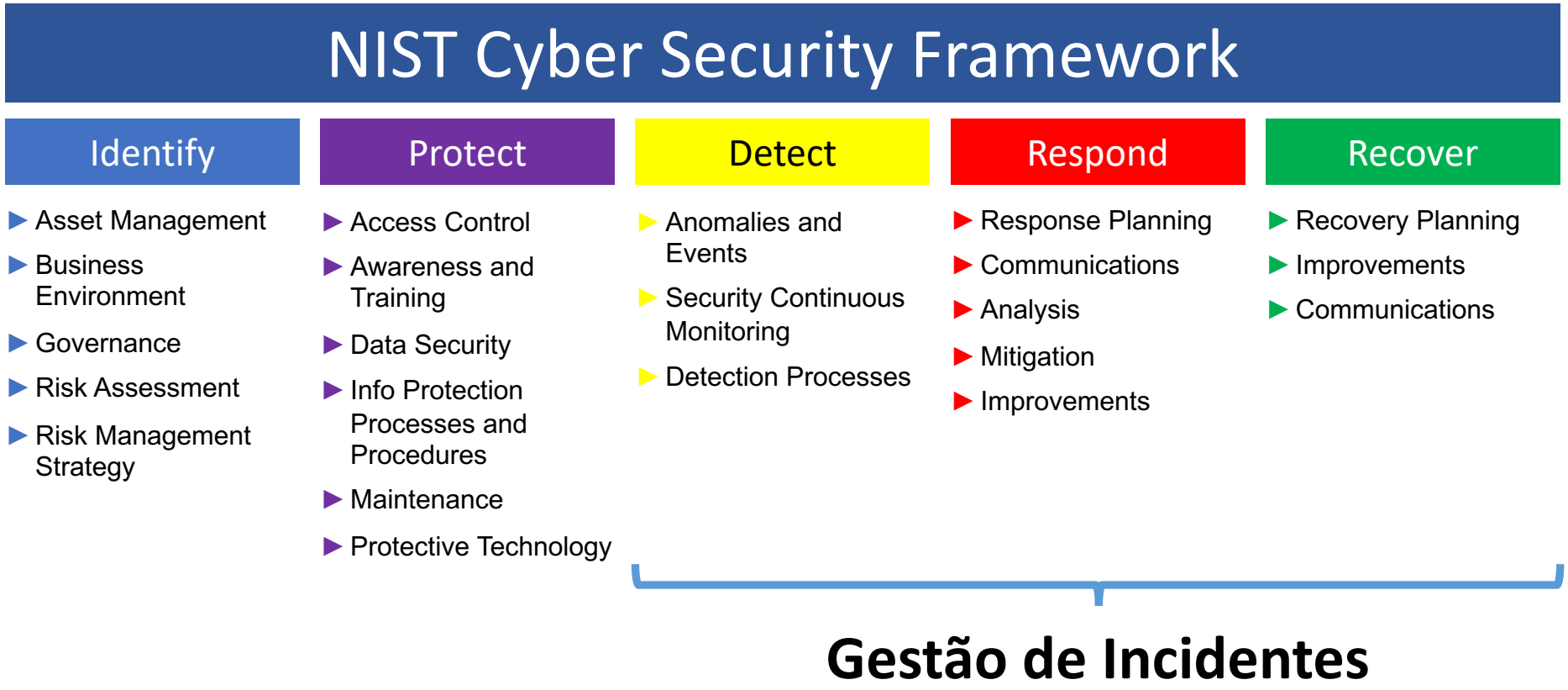
Será utilizado pelo CERT.br a partir de 2024

- Em alinhamento com TF-CISRT
  - Acreditação
  - Certificação

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



Gestão de Riscos, de Segurança e de Incidentes se Complementam



Original em Inglês e tradução para o Português disponíveis em:
https://www.nist.gov/cyberframework/framework
https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf

Relembrando por que precisamos CSIRTs: **Organizações Precisam Alcançar Resiliência**

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

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

O que faz diferença

- **Foco em pessoal**
  - **Profissionais** capacitados e atualizados
  - **Treinamento e conscientização dos usuários**
- **Gestão de Risco**
- **Gestão de Segurança**
- **Gestão de Incidentes**
  - **Formalizar Times de Tratamento de Incidentes de Segurança (CSIRTs)**

Causas Mais Comuns de *Ransomware* e Vazamentos de Dados

Ataques mais reportados ao CERT.br e mais observados em nossos sensores:

- Acesso indevido via **senhas fracas** ou **comprometidas/vazadas**, incluindo
  - *Phishing*
  - Senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas
  - Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
    - *e-mails* e serviços em nuvem
    - acesso remoto (VPN, SSH, RDP, Winbox, etc)

- Exploração de **vulnerabilidades antigas** para invasão e/ou movimentação lateral
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

Portal de Estatísticas do CERT.br
https://stats.cert.br/

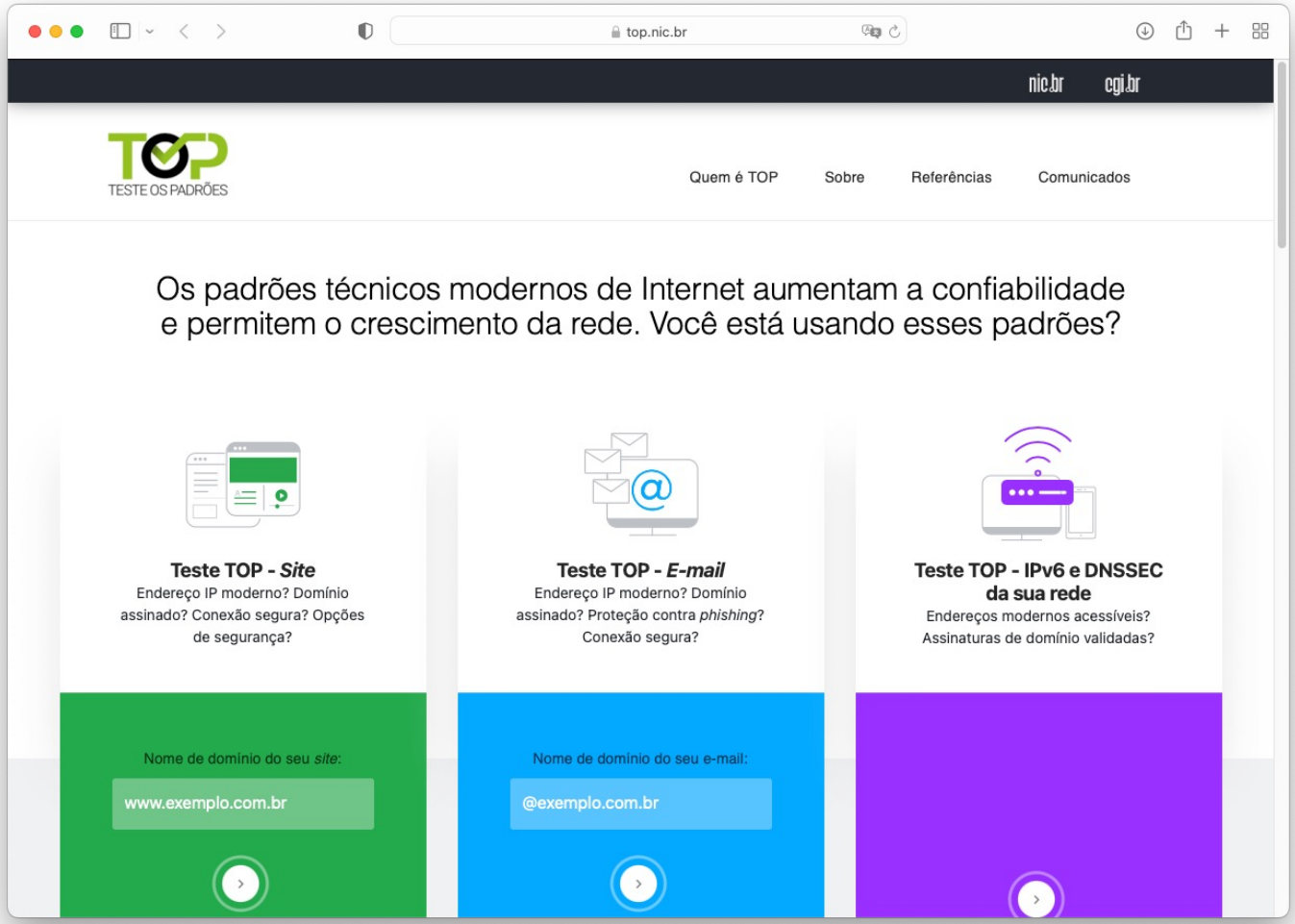
Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- todos os serviços tivessem 2FA / MFA
- houvesse mais atenção a erros e configurações

Barreiras para melhoria: formação dos profissionais e priorização por gestores

Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras
Autores: NIC.br (CERT.br e Cetic.br), em parceria com OECD
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Aumentar a segurança de serviços expostos: **Protocolos modernos e seguros para *sites*, *e-mail* e conectividade**



https://top.nic.br/

Testa a correta implementação de

- IPv6
- DNSSEC
- TLS e cifras
- SPF / DKIM / DMARC
- STARTTLS / DANE

Testes

- verificam a correta implementação dos padrões
- baseiam-se
  - nas especificações das RFCs
  - em padrões técnicos operacionais recomendados por entidades internacionais

Relatório

- detalhamento de todos os resultados
  - referências sobre os padrões
  - dicas sobre como corrigir possíveis problemas

TLP:CLEAR

notificações para: cert@cert.br @certbr

https://cert.br/

https://cartilha.cert.br/

https://InternetSegura.br/

nic.br cgi.br

www.nic.br | www.cgi.br