

nic.br egi.br

cert.br

Seminário Internacional de Segurança Cibernética nas Cortes Superiores

Supremo Tribunal Federal

25 de agosto de 2023

Brasília, DF

Serviços Prestados à Comunidade

Gestão de Incidentes

- ▶ Coordenação
- ▶ Análise Técnica
- ▶ Suporte à Mitigação e Recuperação

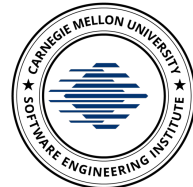
Consciência Situacional

- ▶ 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:



SEI
Partner
Network



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

Boas Práticas para Gestão de Incidentes Cibernéticos

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

TLP conforme padrão do FIRST

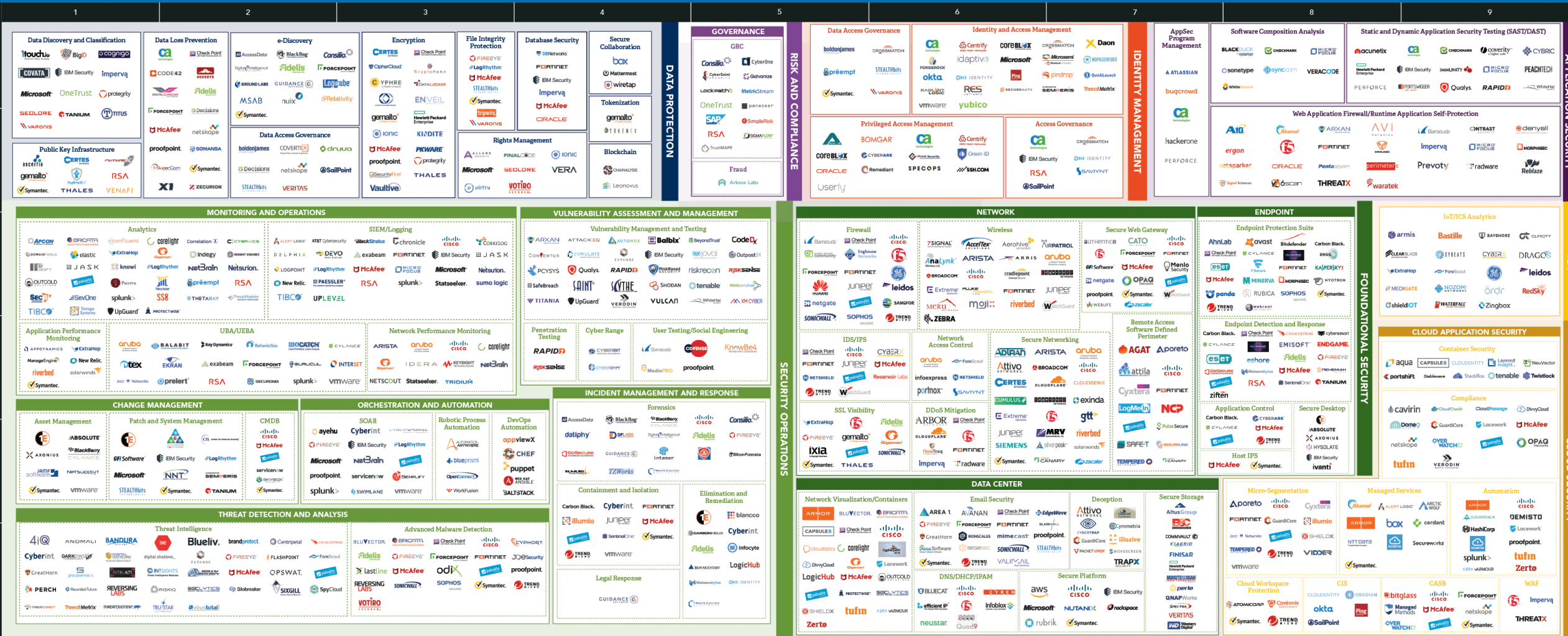
<https://cert.br/tlp/>

Slides *online* em

<https://cert.br/docs/palestras/>

cert.br nic.br egi.br

Optiv Cybersecurity Technology Map



Navigating the Security Landscape
 So much technology. So many vendors. Who does what?

<https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers>



Com tantas soluções, o problema está resolvido, certo?

200+

Median number of days
attackers are present on
a victims' network
before detection

80

Days after detection
to full recovery

\$3Trillion

Impact of lost
productivity and growth

\$3.9Million

Average cost of a data
breach (15% YoY
increase)

Fonte:

RSA Conference 2022, Session ID: HTA-M05, Strong Story to Tell: Top 10 Mistakes by Administrators About Remote Work
Paula Januszkiewicz, CEO, Cybersecurity Expert - CQURE Inc.

O que esses números significam?

Há problemas na detecção

- falta de pessoal interno capacitado para
 - personalizar configurações
 - entender alertas
- ferramentas não funcionam sem processos e integração adequadas

Recuperação é lenta e cara

- demora na detecção leva a
 - impactos mais sérios
 - mais dados e ativos comprometidos
- recuperação é difícil na falta de
 - pessoal capacitado
 - processos e papéis bem definidos

200+

Median number of days
attackers are present on
a victims' network
before detection

80

Days after detection
to full recovery

\$3Trillion

Impact of lost
productivity and growth

\$3.9Million

Average cost of a data
breach (15% YoY
increase)

Fonte:

RSA Conference 2022, Session ID: HTA-M05, Strong Story to Tell: Top 10 Mistakes by Administrators About Remote Work

Paula Januszkiewicz, CEO, Cybersecurity Expert - CQURE Inc.

You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

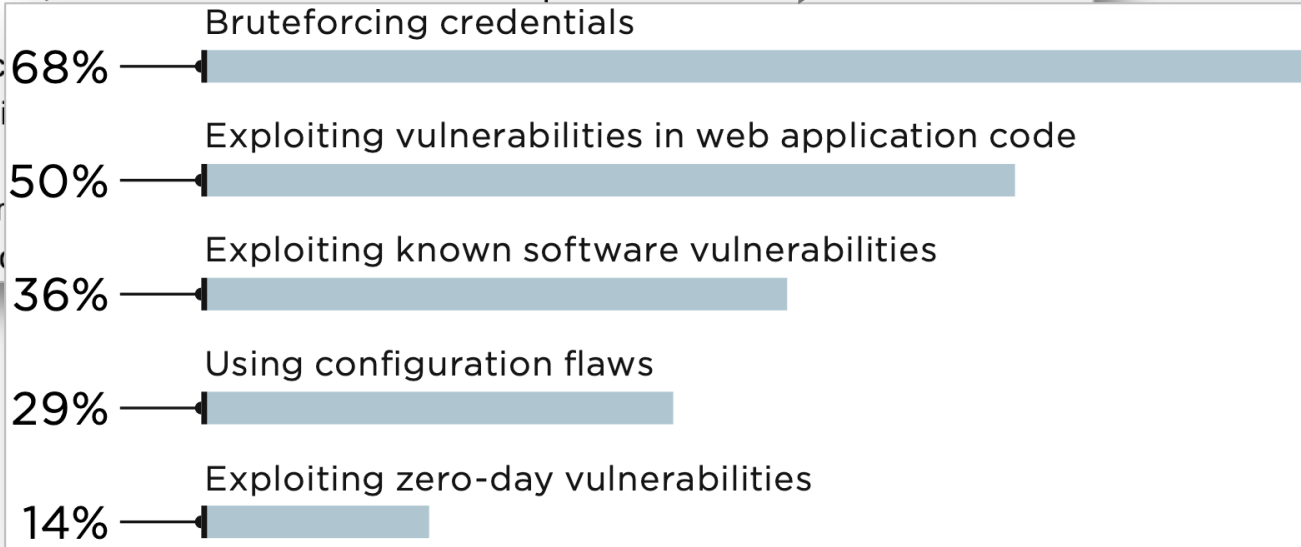
Three little words: Patches, passwords, policies

Thu 13 Aug 2020 // 07:06 UTC

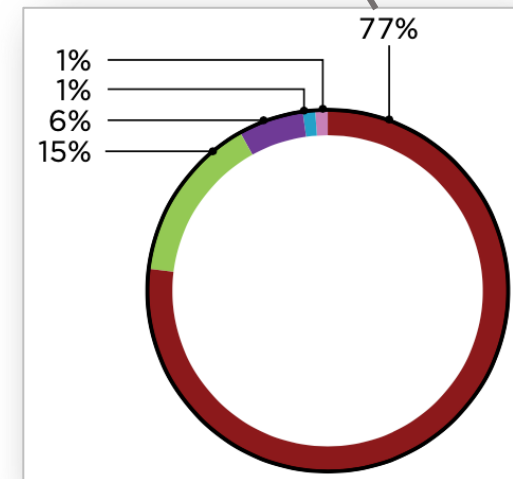
Shaun Nichols in San Francisco [BIO](#) [EMAIL](#) [TWITTER](#)

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

This is according to a recent survey by Technology Research Associates and found that 77% of its red team members have found vulnerabilities available to the public.



- Using web application protection vulnerabilities and flaws
- Bruteforcing credentials used for accessing DBMS
- Bruteforcing credentials for remote access services
- Bruteforcing domain user credentials together with software vulnerabilities exploitation
- Bruteforcing credentials for the FTP server



31

https://www.theregister.com/2020/08/13/pentest_networks_fail/

<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf>

Causas Mais Comuns de Invasões 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
 - 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)
 - gestão remota de ativos de rede e servidores
- 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/>

Mas existem os outros 20% dos incidentes

Organizações Precisam Alcançar Resiliência

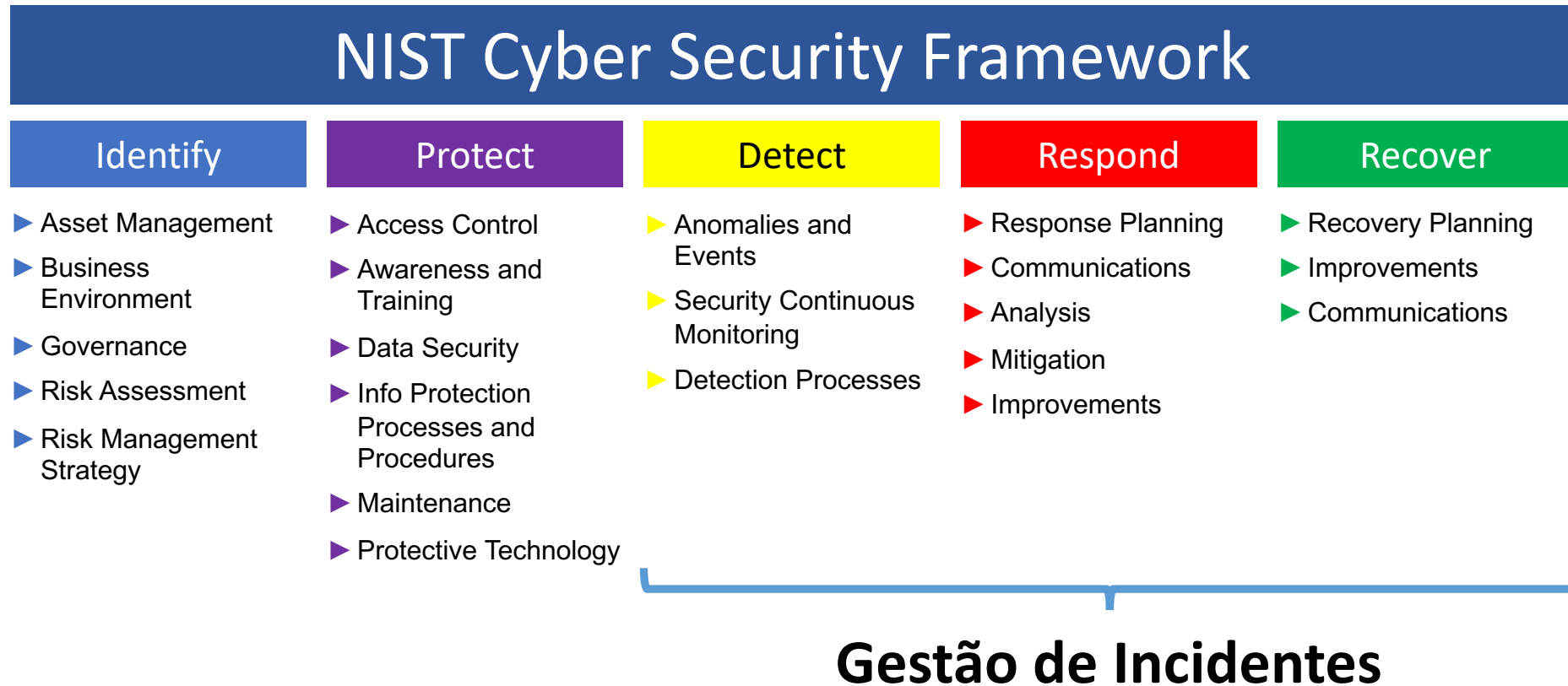
Um sistema 100% seguro é impossível de atingir: incidentes ocorrerão

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 - do Inglês *Computer Security Incident Response Teams*)**

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

CSIRTs Efetivos

cert.br nic.br egi.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

FIRST - *Forum of Incident Response and Security Teams*

- Fórum Global que reúne mais de 687 times de 106 países

CSIRTs

Evolução e Desafios

Número crescente

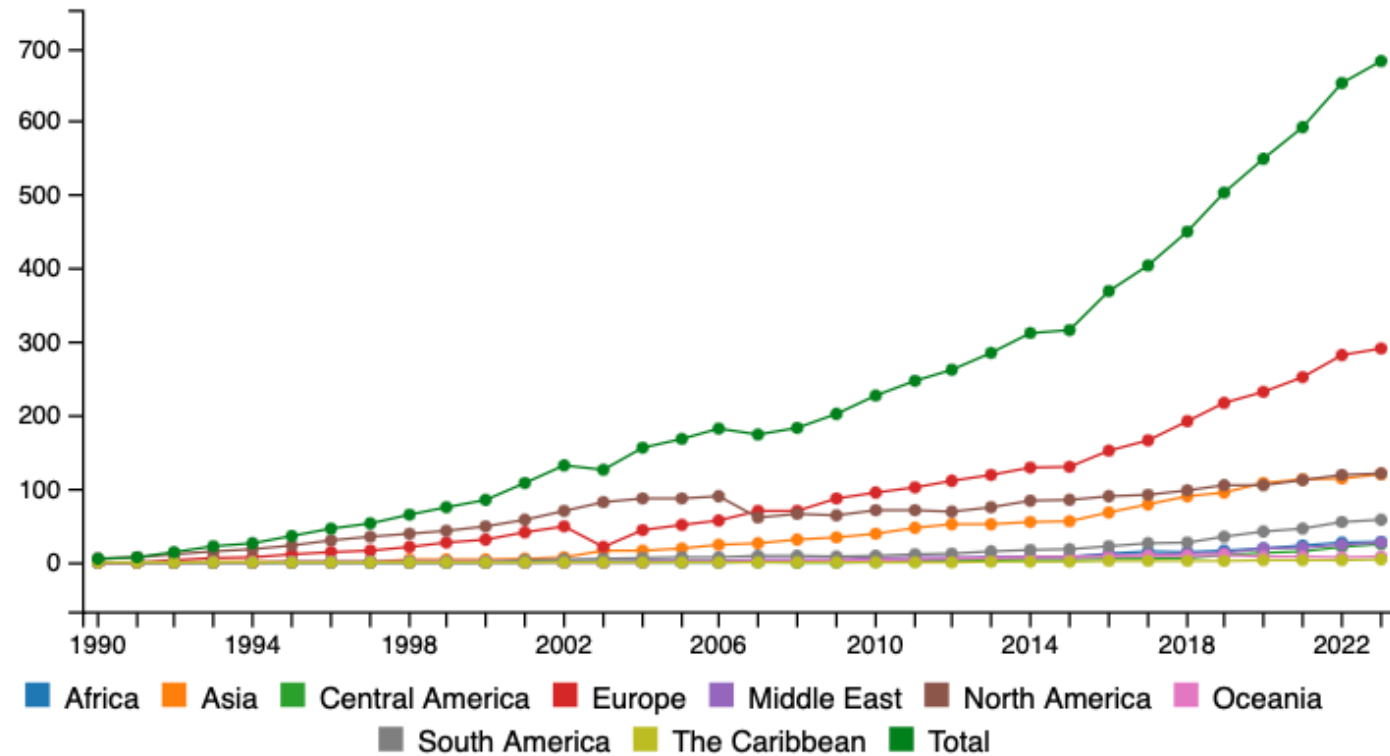
- Diversos países
- Diversos setores
- Variados níveis de maturidade

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?

FIRST members growth by year*



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

Fonte: FIRST History, link visitado em 23/08/2023

<https://www.first.org/about/history>

Padrões de Serviços e Maturidade Essenciais para um CSIRT Efetivo

Padrões

- 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*)
- *Open CSIRT Foundation*
 - **SIM3 (Security Incident Management Maturity Model)**

Organizações envolvidas

- FIRST – *Forum of Incident Response and Security Teams*
 - SIGs (*Special Interest Groups*) e Comitês
- *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

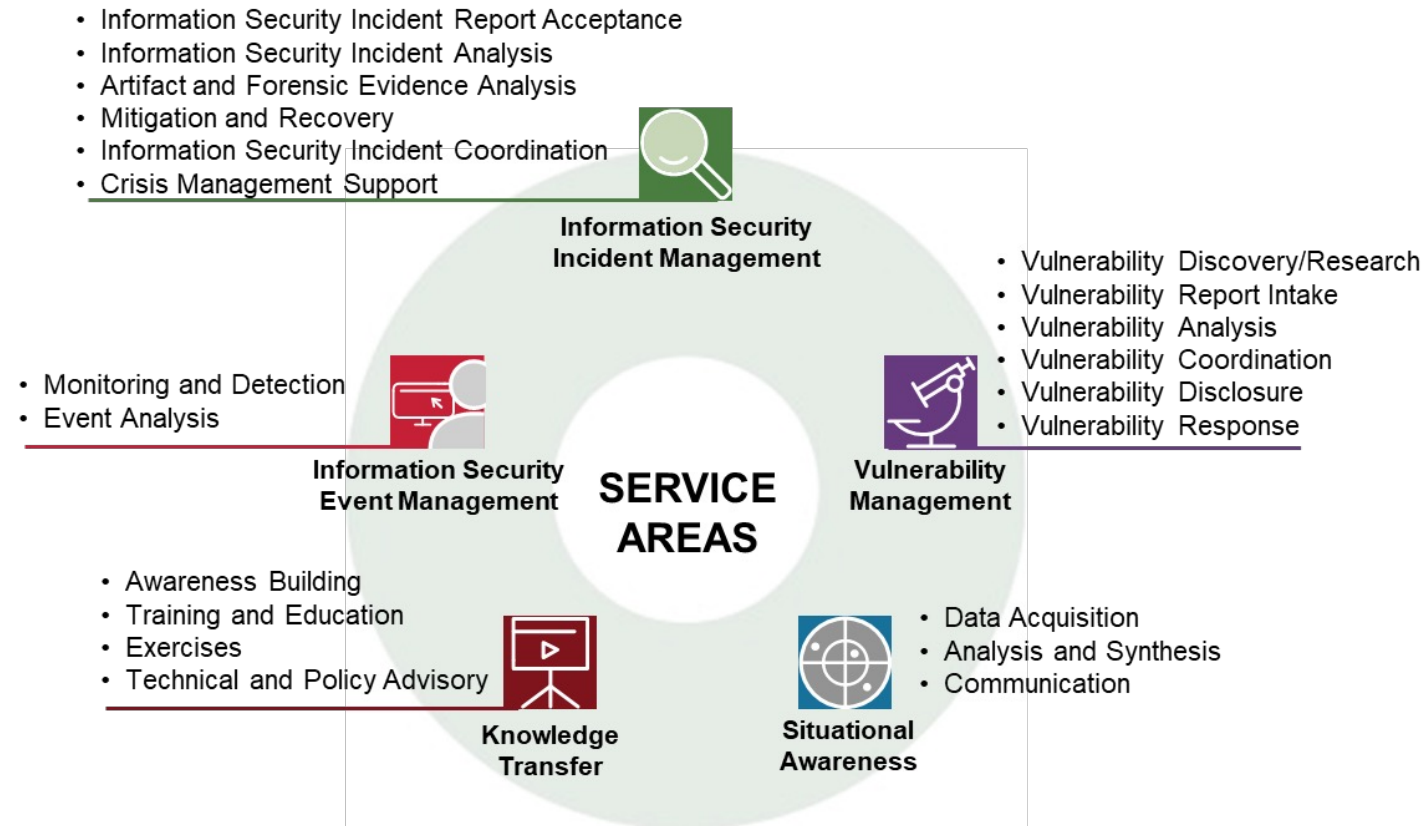
- por um CSIRT
- por times com serviços relacionados com gestão de incidentes

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

SIM3 – Security Incident Management Maturity Model

Quatro pilares

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

Quatro quadrantes

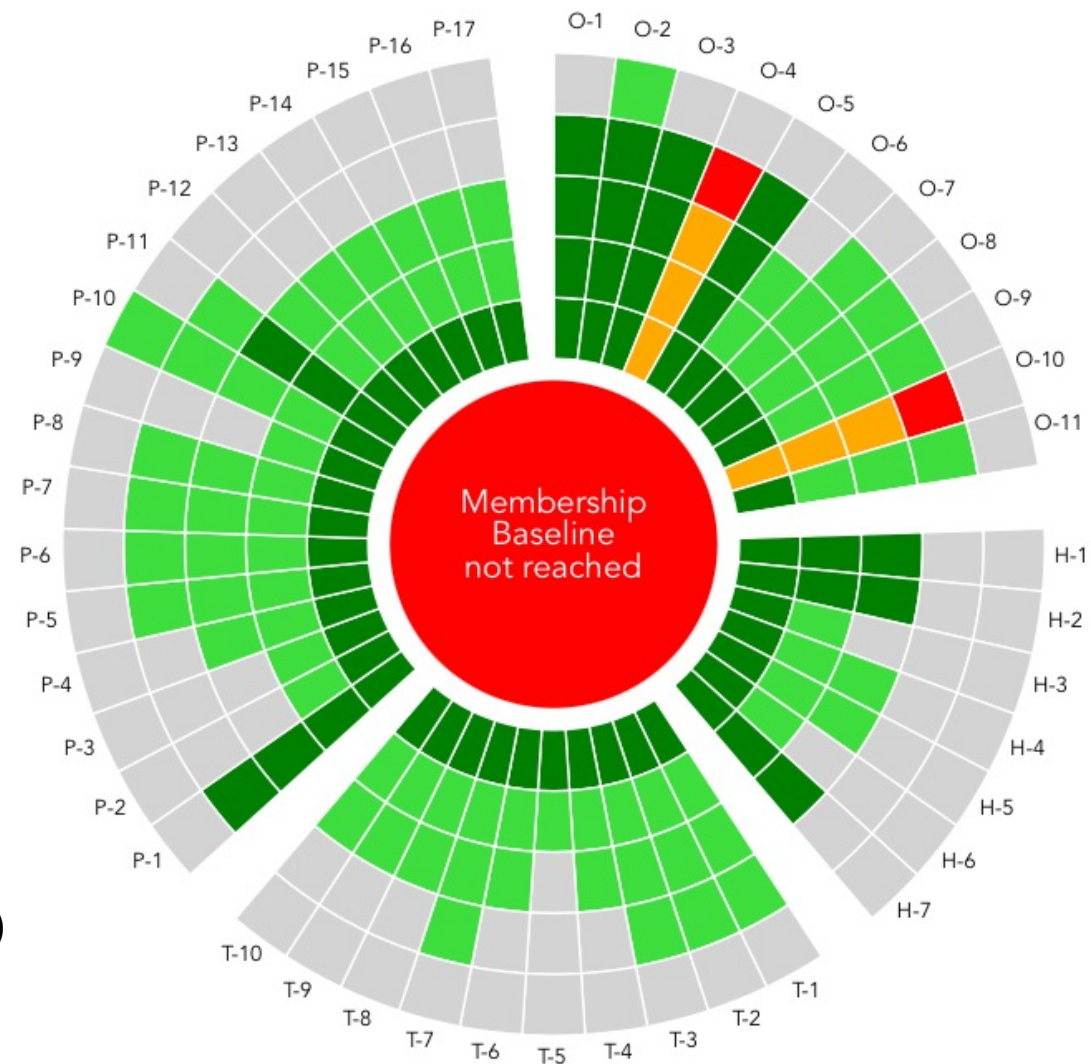
- O – *Organisation* (11 parâmetros)
- H – *Human* (7 parâmetros)
- T – *Tools* (10 parâmetros)
- P – *Processes* (17 parâmetros)

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/>



powered by OpenCSIRT SIM3-check

Auto avaliação SIM3 Online Tool

Em forma de perguntas

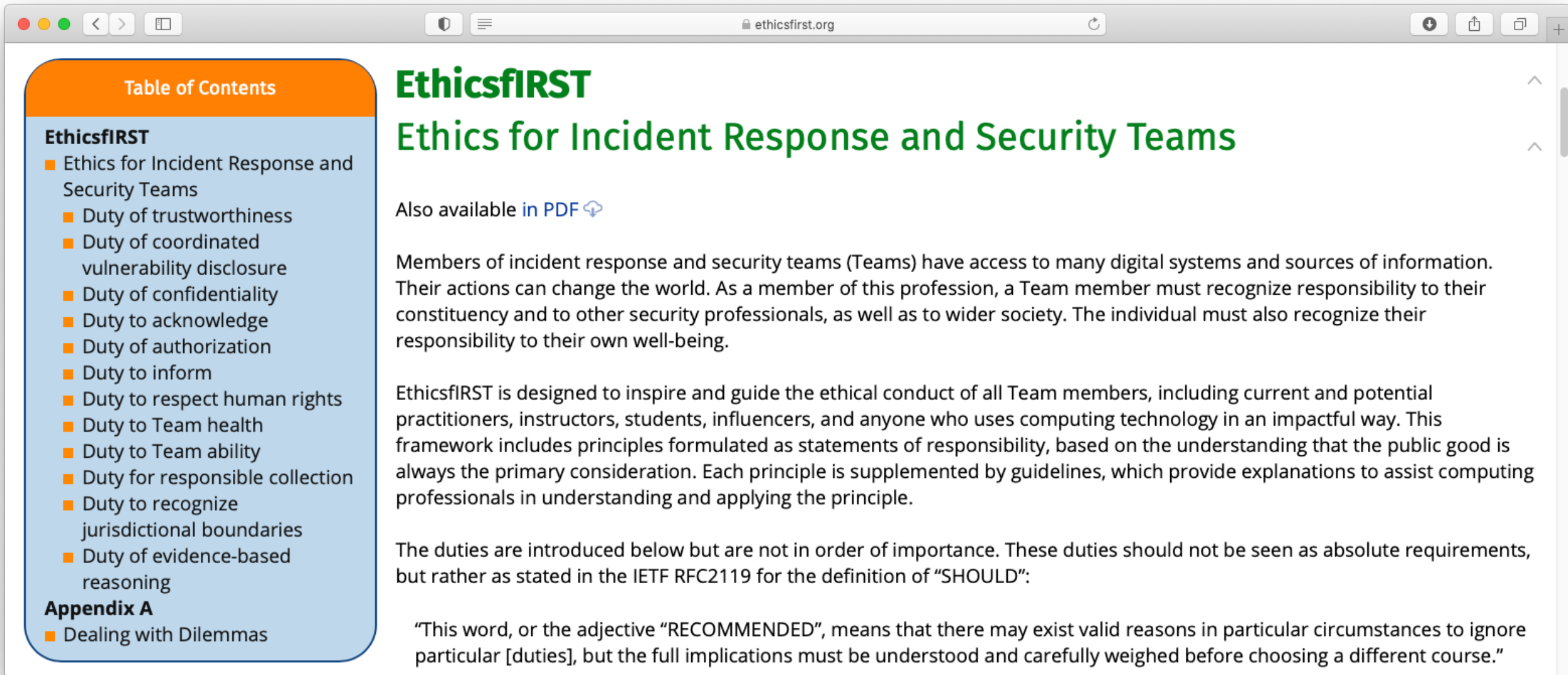
Possui 4 perfis

- 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/>



The screenshot shows a web browser window with the address bar displaying "ethicsfirst.org". The page content is as follows:

Table of Contents

- EthicsFIRST**
 - Ethics for Incident Response and Security Teams
 - Duty of trustworthiness
 - Duty of coordinated vulnerability disclosure
 - Duty of confidentiality
 - Duty to acknowledge
 - Duty of authorization
 - Duty to inform
 - Duty to respect human rights
 - Duty to Team health
 - Duty to Team ability
 - Duty for responsible collection
 - Duty to recognize jurisdictional boundaries
 - Duty of evidence-based reasoning
- Appendix A**
 - Dealing with Dilemmas

EthicsFIRST

Ethics for Incident Response and Security Teams

Also available [in PDF](#)

Members of incident response and security teams (Teams) have access to many digital systems and sources of information. Their actions can change the world. As a member of this profession, a Team member must recognize responsibility to their constituency and to other security professionals, as well as to wider society. The individual must also recognize their responsibility to their own well-being.

EthicsFIRST is designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. This framework includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

The duties are introduced below but are not in order of importance. These duties should not be seen as absolute requirements, but rather as stated in the IETF RFC2119 for the definition of "SHOULD":

"This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore particular [duties], but the full implications must be understood and carefully weighed before choosing a different course."

Relembrando

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 - do Inglês *Computer Security Incident Response Teams*)**

Obrigada

📧 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