

nic.br egi.br

cert.br

**Como Se Prevenir E Atuar Durante Um Incidente De Segurança**

**13 de Julho de 2022**

**Evento Online**

*Live Intra Rede*

# Gestão de Incidentes

Lucimara Desiderá, M.Sc  
Analista de Segurança  
lucimara@cert.br

cert.br nic.br egi.br

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

## Ataques mais reportados e mais observados 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

## Mais de 80% dos incidentes seriam evitados se

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

Estudo Setorial

Segurança digital: uma análise de gestão de risco em empresas brasileiras

<https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/>

Você teria um conselho para as empresas para reduzir o número de incidentes?

**“Multifactor Everything”**

-- Katie Moussouris (Luta Security, US)

<https://youtu.be/4tuC32PlyJk>

## Fontes:

Principais Ataques na Internet: Dados do CERT.br

<https://youtu.be/nHh8hHaomFE?t=714>

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

# É Possível Segurança 100%?

## 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](http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html)



# 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, Dados e Pessoas)



## 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

É possível:

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

# Incidentes Ocorrerão: 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.)
- **Implantar medidas de segurança** que implementem as políticas de segurança
  - ex: aplicar correções ou instalar ferramentas de segurança
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- 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

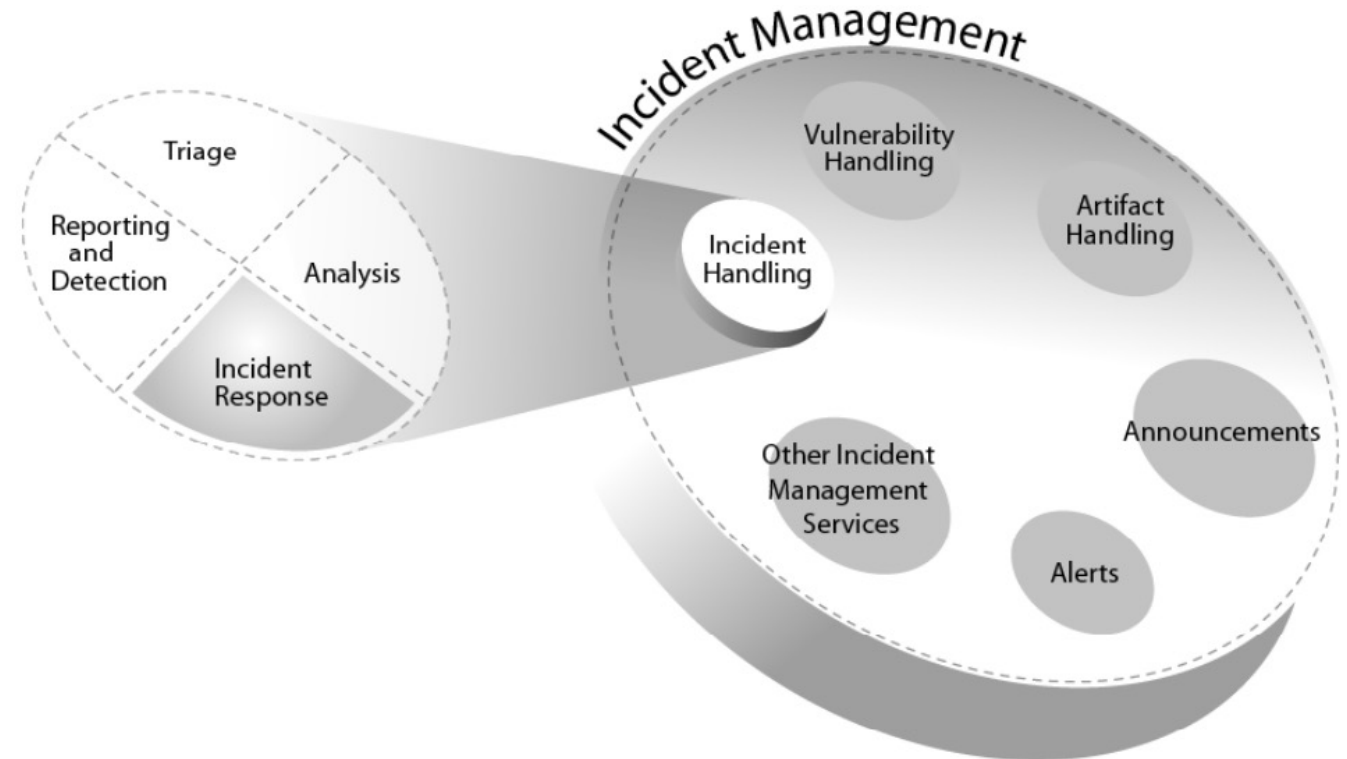
- gestão fim a fim de eventos e incidentes
- envolve toda a organização

## 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

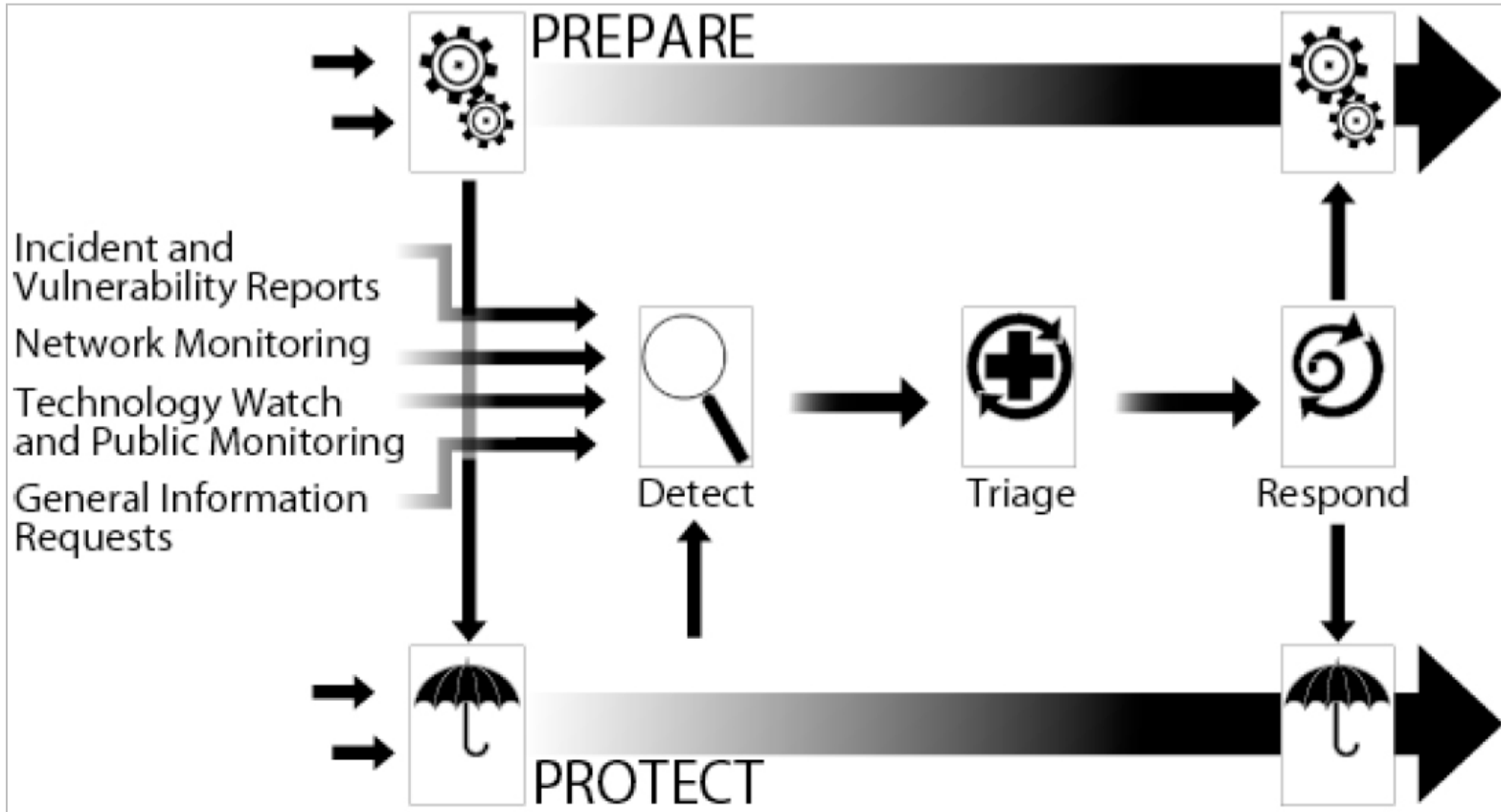
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT

## 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>



# Análise do Incidente e Fluxos de Tratamento

## Dia-a-dia da Equipe de Tratamento:

- identifica e trata vários incidentes, seguindo o processo mostrado anteriormente
- o processo inclui a análise do incidente e a identificação de
  - escopo e natureza
  - se há necessidade de resposta gerencial
    - esta identifica se é necessária resposta legal
    - a resposta legal é requerida, por exemplo
      - se for identificado crime,
      - quebra de contrato
      - incidente que envolva dados pessoais e que possa acarretar risco ou dano relevante aos titulares
  - em todos estes casos é necessário seguir normas e legislação pertinentes a cada setor/órgão

## Em outras palavras:

Do ponto de vista de uma empresa/instituição, o fluxo de de tratamento de incidentes envolvendo dados pessoais deve se diferenciar apenas na fase final.

Por exemplo:

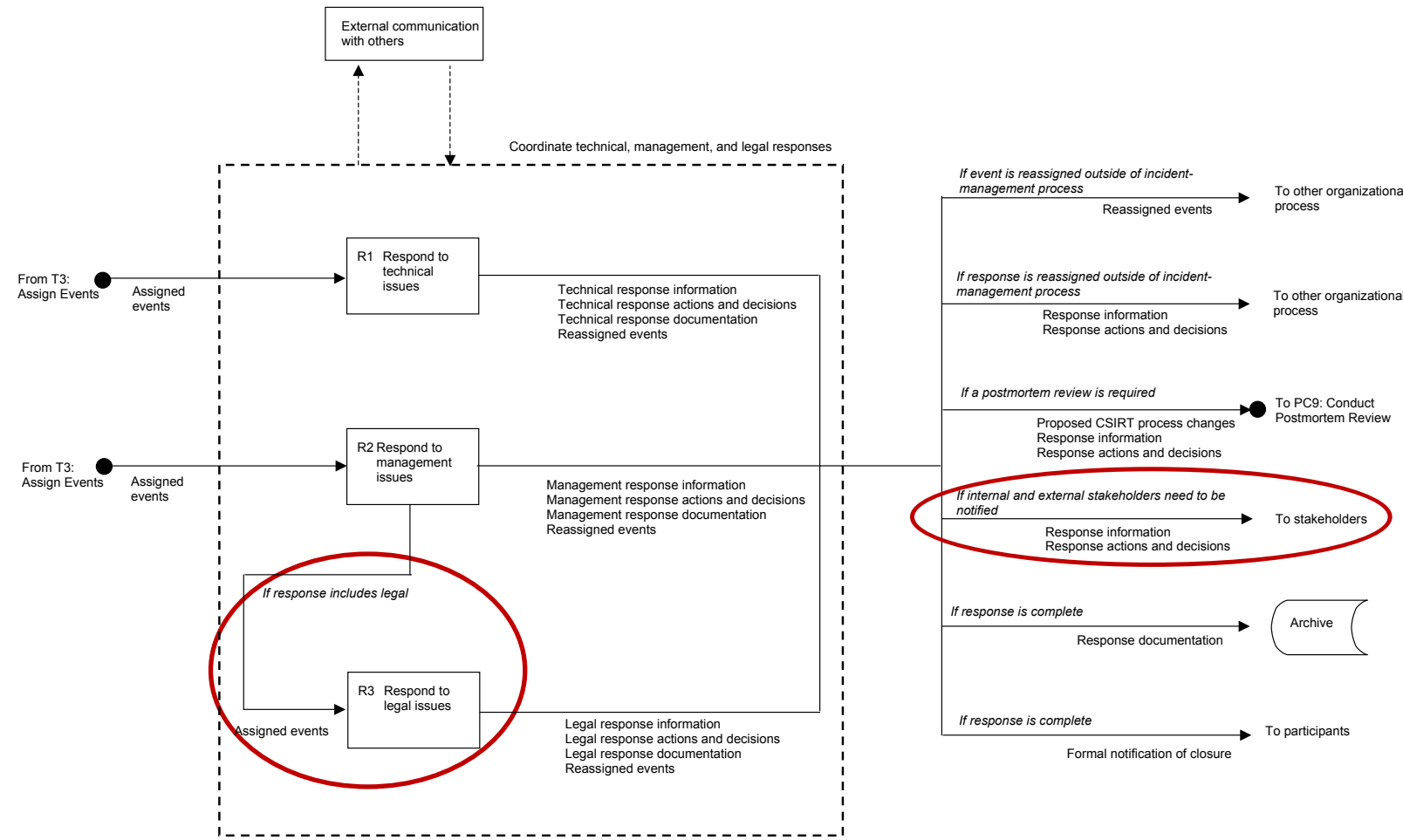
1. Incidente é detectado
2. Análise mostra que quebrou um contrato?
  - se sim, aciona jurídico para providências
3. Análise mostra que é crime?
  - se sim, aciona jurídico para avaliar se necessita notícia aos operadores da justiça
4. Análise mostra que afetou dados pessoais?
  - se sim, aciona jurídico para avaliar se necessita envio de relatório para a ANPD

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.

# Tratamento de Incidentes Envolvendo Dados Pessoais: Tipos de Resposta no Fluxo de Tratamento de Incidentes

Existe mais de um tipo de resposta que pode ser dada a um incidente de segurança

- a **resposta legal** é uma decisão de cunho **gerencial**
  - uma equipe técnica não pode, por via de regra, iniciar sozinha uma resposta legal, como a notificação a uma Autoridade ou Agência reguladora
- a **resposta técnica** ao incidente ocorre em paralelo à resposta gerencial e segue tempos diferentes
- a ANPD é um dos *stakeholders* externos a ser notificado, como parte normal do processo



Fonte: *Defining Incident Management Processes for CSIRTs: A Work in Progress*, páginas 152 e 221  
<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153>

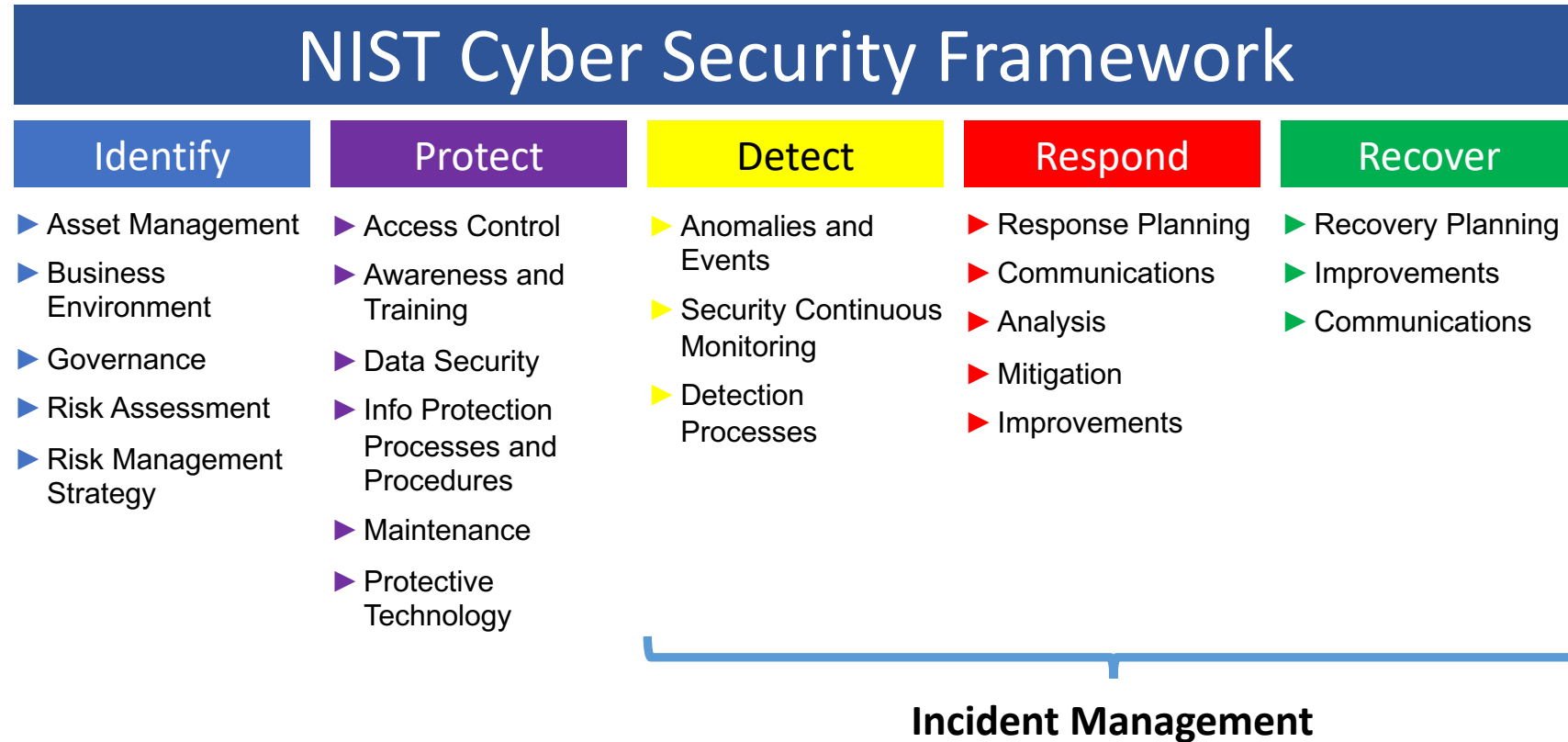
# Gestão de Incidentes não está Isolada: Pode ser Encontrada em todos os *Frameworks*

*“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.”*



Original em Inglês e tradução para o Português disponíveis em:

<https://www.nist.gov/cyberframework/framework>

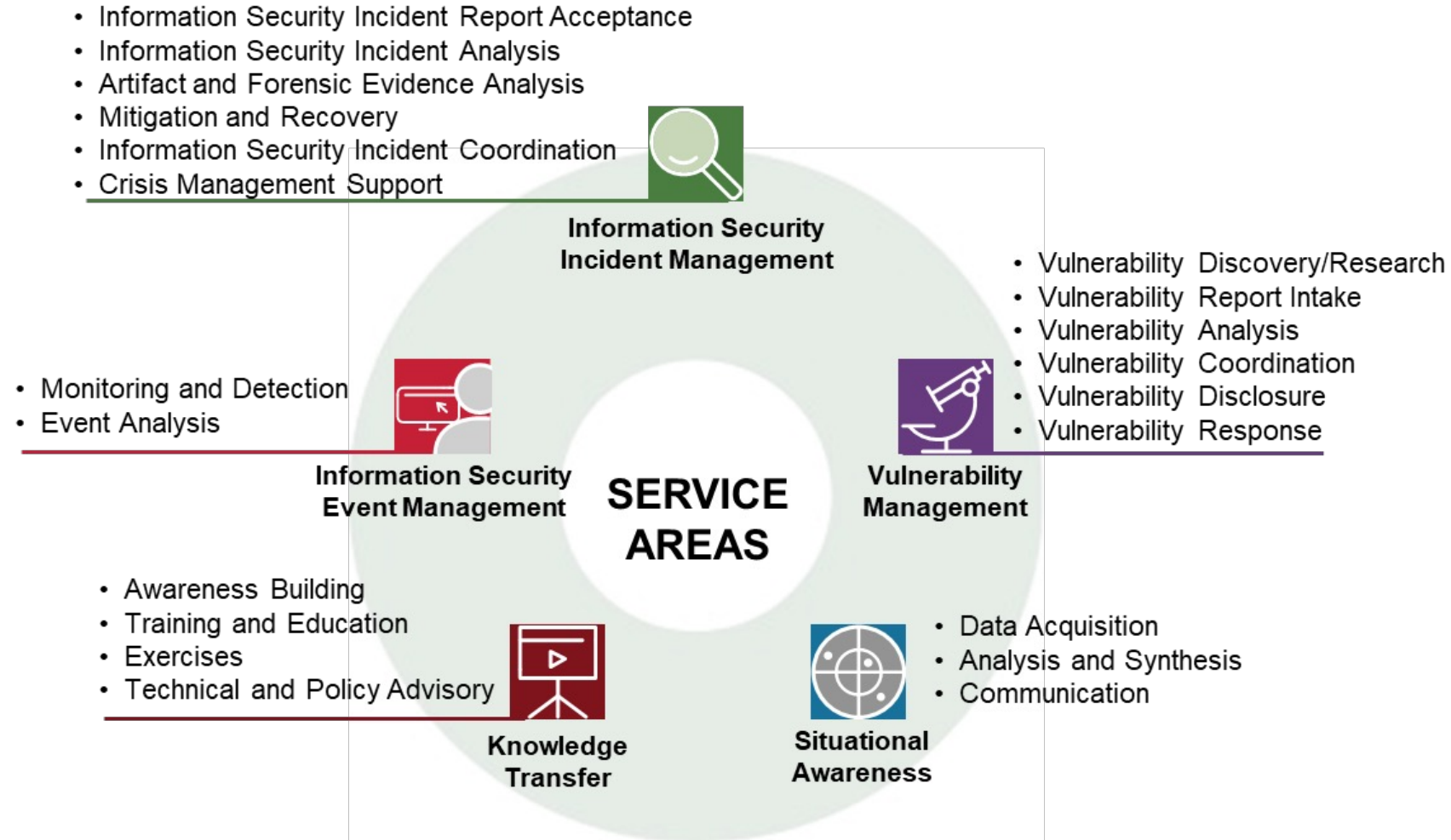
# Gestão de Incidentes: Serviços e Funções

*“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/>



# Referências Adicionais

cert.br nic.br egi.br



# Foco do CERT.br nestes 25 anos: Aumentar a Capacidade Nacional de Tratamento de Incidentes

**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

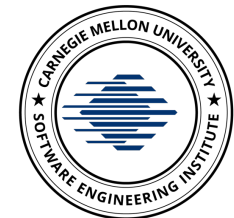
## **Lista de CSIRTs Brasileiros**

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

## **Cursos de Gestão de Incidentes**

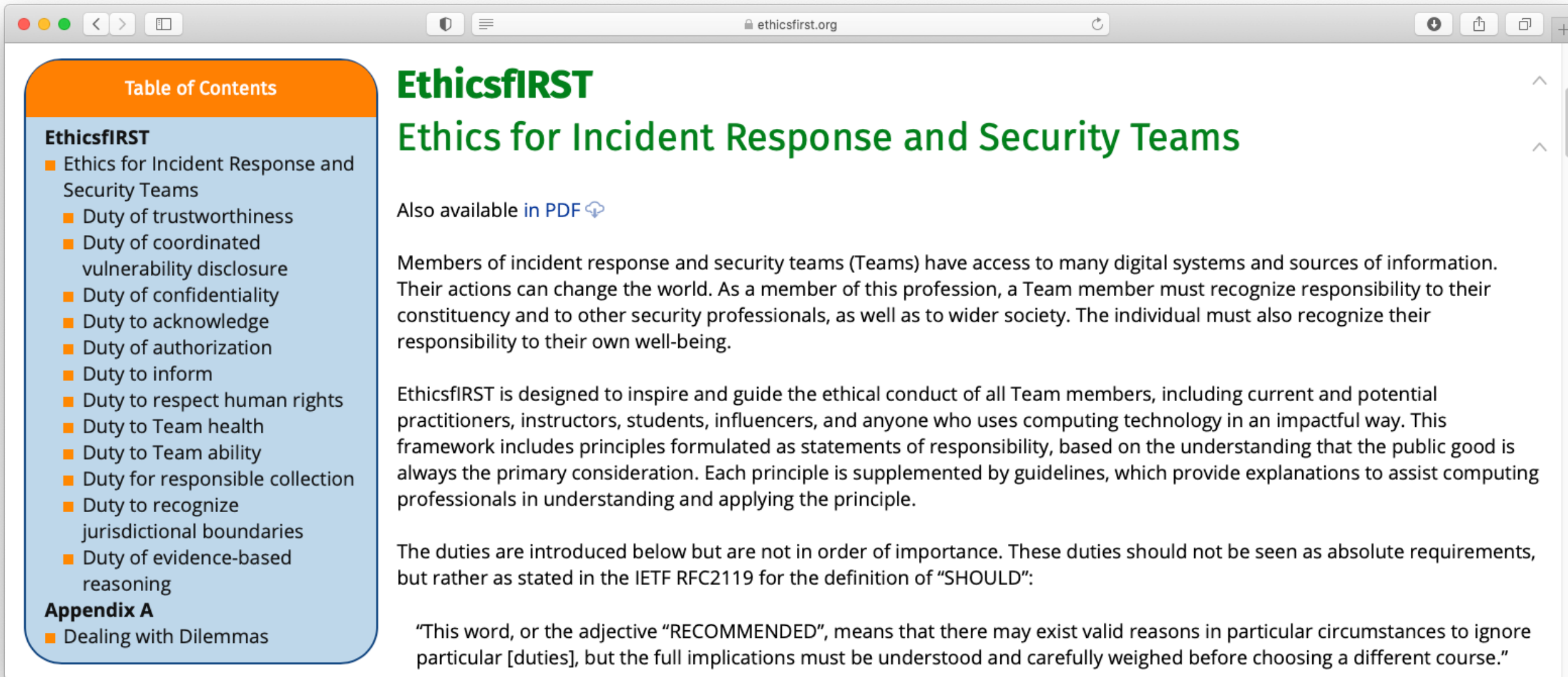
Ministra os cursos do *CERT<sup>®</sup> Division*, do *SEI/Carnegie Mellon*, desde 2004:

- <https://cert.br/cursos/>



**SEI**  
Partner  
Network

# EthicsFIRST.org: Código de Ética da Comunidade Global de CSIRTs




The screenshot shows a web browser window with the URL [ethicsfirst.org](https://ethicsfirst.org). On the left, there is a 'Table of Contents' sidebar with an orange header. The main content area features the title 'EthicsFIRST' in green, followed by the subtitle 'Ethics for Incident Response and Security Teams' also in green. Below the title, there is a link 'Also available in PDF' with a download icon. The main text consists of three paragraphs: an introductory paragraph about the responsibilities of incident response and security teams, a paragraph explaining the purpose of the EthicsFIRST framework, and a paragraph about the importance of the 'SHOULD' term as defined in IETF RFC2119. A quote is provided at the bottom of the main text.

**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.”

# 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 Incident Management Maturity Model**

SIM3 mkXVIIIb<sup>1</sup>  
Don Stikvoort, 30 March  
(b version 1 September 2018)

© Open CSIRT Foundation (OCF) 2016-2018  
S-CURE by 2008-2018 & PRESECURE G.  
The GEANT Association and SURF.  
unlimited right-to-use providing authorisation statement are reproduced; changes of holders OCF, S-CURE and PRESECURE.

Thanks are due to the TI-CERT "certificatie", Droz, chair, Gorazd Bozic, Mirek Maj, Uwe Peter Kowalski, 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 \_\_\_\_\_

<sup>1</sup> In the "b" version of SIM3 mkXVIII, links to external sources have been updated.  
© 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  
■ compliant with the reference

© Open CSIRT Foundation et al. 2008-2018 SIM3 mkXVIIIb p4 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/>

The screenshot displays the SIM3 Self Assessment Tool interface. The browser address bar shows the URL [sim3-check.opencsirt.org](https://sim3-check.opencsirt.org). The page header includes the Open CSIRT Foundation logo and navigation links for 'Open CSIRT Foundation', 'Help', 'License', and 'Color Scheme'. The main content area is divided into three tabs: 'Organisation', 'Human' (selected), and 'Tools', 'Processes'. The 'Human' tab contains a description of the 'Human' category and a list of questions. The first question, 'H-1: Code of Conduct/Practice/Ethics', is expanded, showing a list of four options. The third option, 'We have a written code of conduct approved by our team management.', is highlighted in orange. The second question, 'H-2: Personnel Resilience', is partially visible. On the right side, the 'Your SIM3 Assessment URL' is displayed, along with a list of four profiles: 'ENISA/GCMF Basic', 'ENISA/GCMF Intermediate', 'ENISA/GCMF Advanced', and 'TI Certification' (highlighted in orange). Below the profiles, there are three buttons: 'Spider-Chart/Show questions', 'Table of Results', and 'Open Actions [7]'. A radar chart is shown at the bottom right, with a central red circle indicating 'TI Certification not reached'. The chart has 17 segments labeled P-1 through P-17 and O-1 through O-11, with various colors representing different assessment levels.

# Obrigada

✉ lucimara@cert.br

✉ notificações para: cert@cert.br

🌐 @certbr

<https://cert.br/>

nic.br cgi.br

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)