

nic.br egi.br

cert.br

**Workshop Incidentes de Segurança de Dados Pessoais**  
**Fórum da Internet no Brasil (FIB) | Pré-IGF Brasileiro**  
28 de julho de 2021 | Evento *Online*

# Incidentes de Segurança no Contexto da Proteção de Dados

Dra. Cristine Hoepers  
Gerente Geral  
[cristine@cert.br](mailto:cristine@cert.br)

cert.br nic.br egi.br

## Serviços Prestados à Comunidade

### Gestão de Incidentes

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

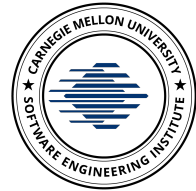
### Consciência Situacional

- ▶ 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 Político

#### Filiações e Parcerias:



SEI  
Partner  
Network



#### Criação:

**Agosto/1996:** CGI.br publica o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”<sup>1</sup>

**Junho/1997:** CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório<sup>2</sup>

<sup>1</sup> <https://cert.br/sobre/estudo-cgibr-1996.html> | <sup>2</sup> <https://nic.br/pagina/gts/157>

## 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

## Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

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

<https://cert.br/sobre/filiacoes/>

<https://cert.br/about/rfc2350/>



# Gestão de Incidentes: Definições Técnicas

**Incidente de Segurança** – cada organização precisa definir o que é um incidente para ela, em geral com base na missão, serviços e recursos disponíveis.

**Notificação de Incidente** – ato informal de reportar a uma rede/empresa a ocorrência de um potencial incidente, normalmente um *e-mail* ou formulário *online*

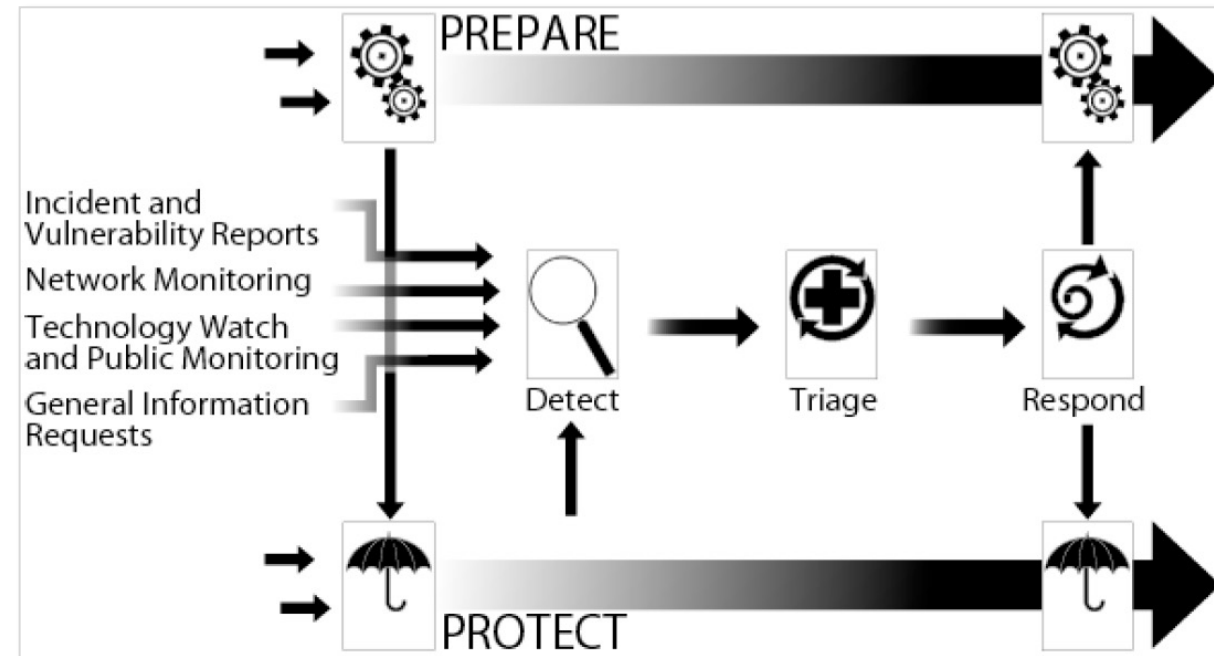
- Foco é pedir/oferecer ajuda
- Requer análise técnica para verificar
  - se é mesmo incidente
  - qual a natureza, escopo e impacto do incidente

**Gestão de Incidentes** – políticas e estratégias

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

**Tratamento de Incidentes** – processos

- prevenir, identificar, mitigar e responder



**Resposta a Incidentes** – ações

- resolver ou mitigar incidentes
- disseminar informações
- implementar estratégias para impedir que o incidente ocorra novamente

**CSIRT** – Equipe de Tratamento de Incidentes de Segurança

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>

# Incidente vs. Vazamento de Dados: Definições Técnicas

**Incidente de Segurança** – cada organização precisa definir o que é um incidente para ela, em geral com base na missão, serviços e recursos disponíveis.

Dois **possíveis exemplos** de definições são:

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

-ou-

O ato de violar uma política de segurança, explícita ou implícita.

Exemplos de incidentes incluem atividades como:

- tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados;
- interrupção indesejada ou negação de serviço;
- uso não autorizado de um sistema para processamento ou armazenamento de dados;
- modificações nas características de *hardware*, *firmware* ou *software* de um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema.

Fonte:

[https://cert.br/certcc/csirts/csirt\\_faq-br.html](https://cert.br/certcc/csirts/csirt_faq-br.html)

**Violação ou Vazamento de Dados (*Data Breach* ou *Data Leak*)**

“Divulgação não autorizada de informações sensíveis para um terceiro, normalmente fora da organização, que não está autorizado a ter ou ver a informação.”

“Vazamentos de dados (*data leak*) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros.”

“Perda de Dados: a exposição de informações proprietárias, sensíveis ou classificadas via furto ou vazamento de dados.”

Fontes:

<https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#D>

<https://cartilha.cert.br/fasciculos/#vazamento-de-dados>

[https://csrc.nist.gov/glossary/term/data\\_loss](https://csrc.nist.gov/glossary/term/data_loss)

# Art. 48 da LGPD reflete casos em que o incidente é descoberto pela própria organização e deve ser notificado à ANPD – Visão do Processo

**Assim como nem todo incidente é crime,  
nem todo incidente envolve dados pessoais.**

## **Dia-a-dia do Agente 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 ou incidente que envolva dados pessoais e que possa acarretar risco ou dano relevante aos titulares
      - neste último caso, um relatório deve ser enviado à ANPD

## **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.

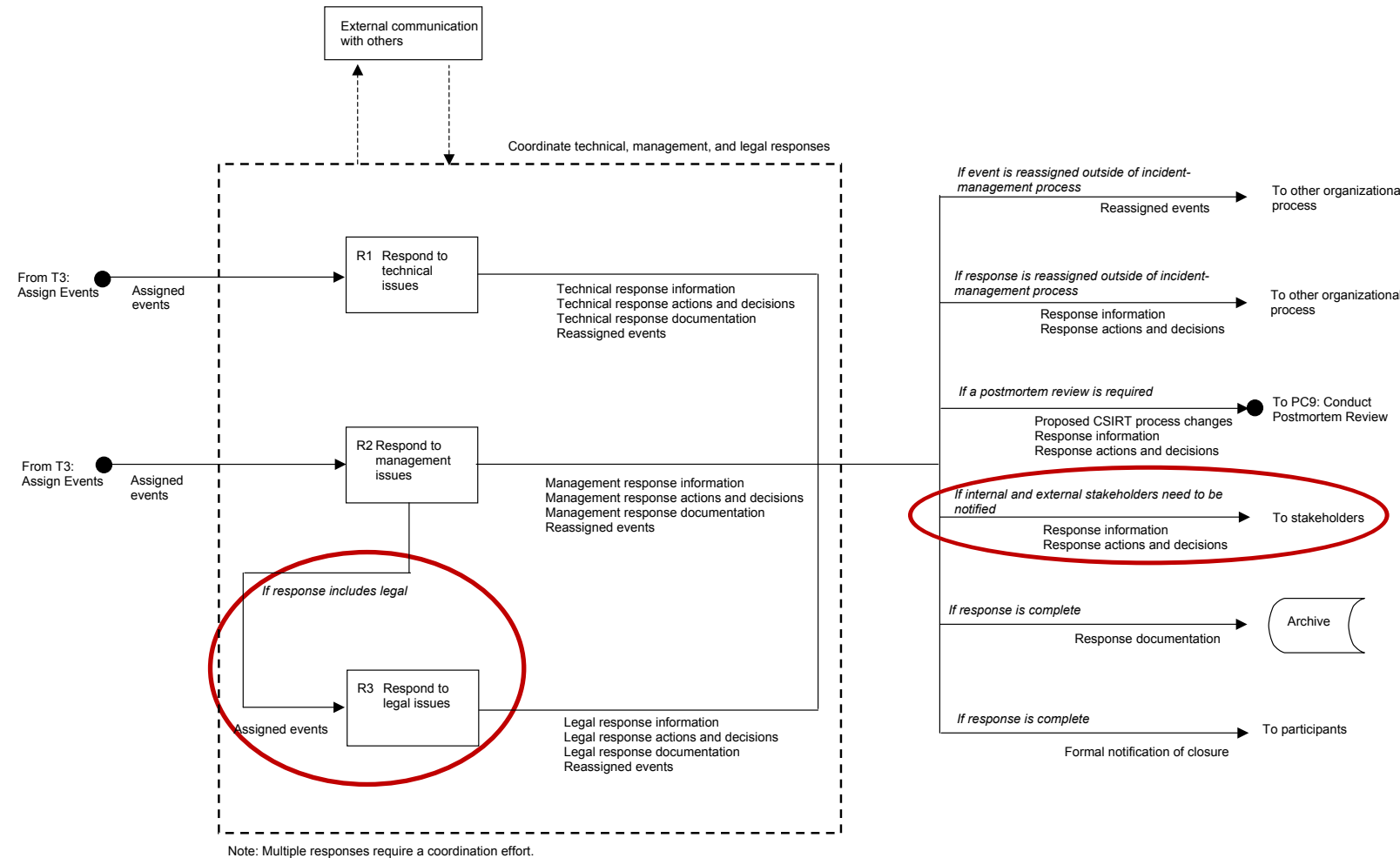
Por exemplo:

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

# 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>

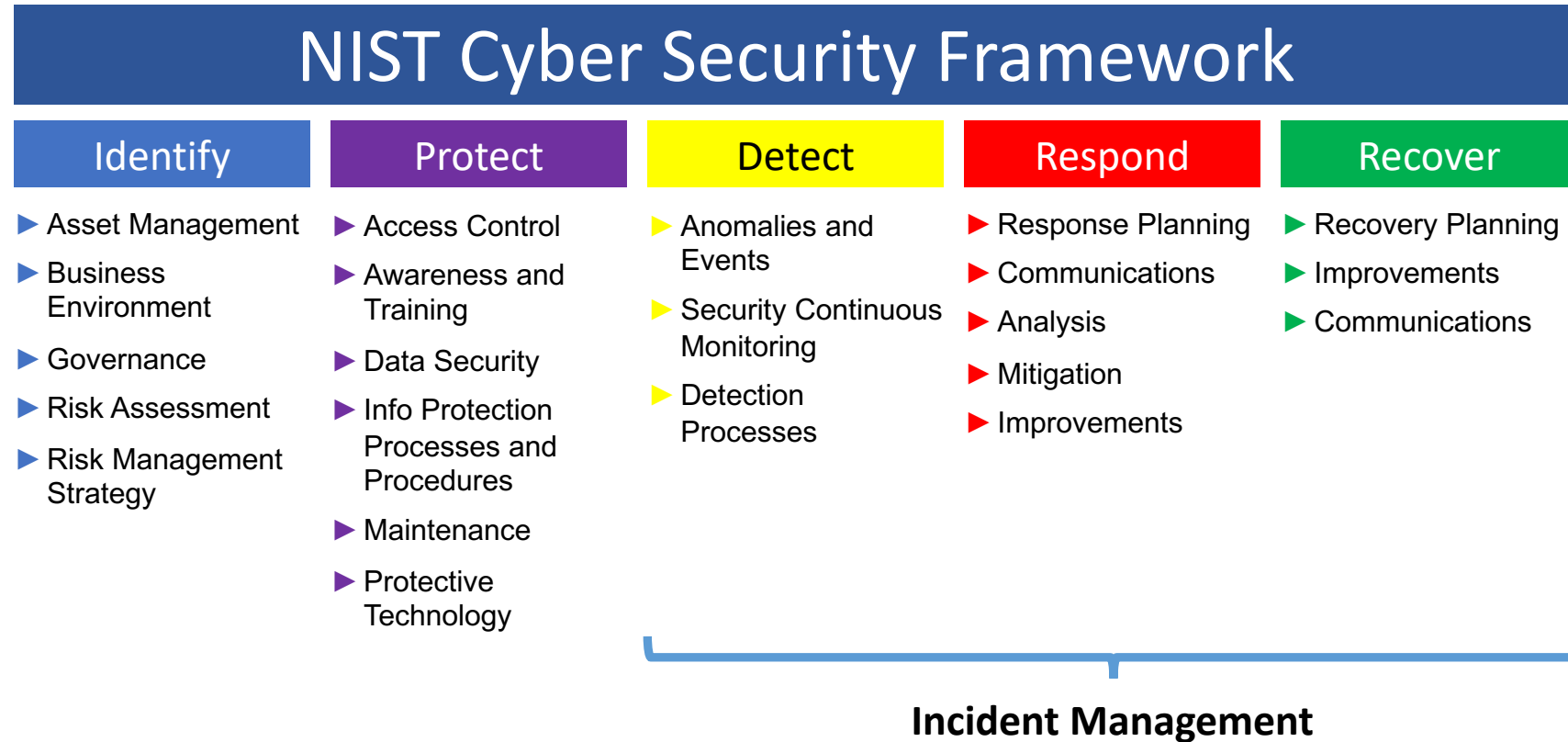
# Gestão de Incidentes não está Isolada: Pode ser Encontrada em Outros *Frameworks*

“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.*”



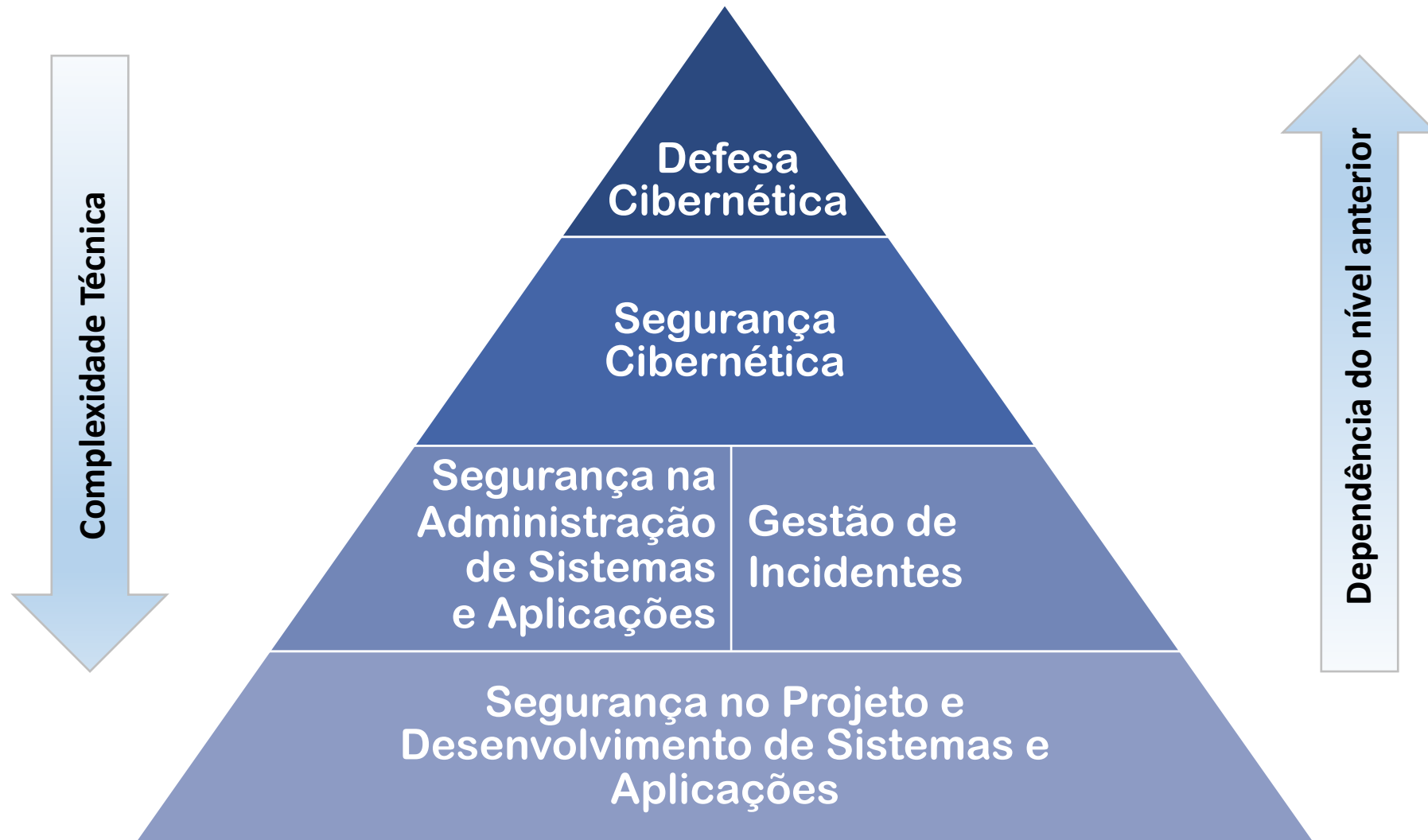
Original em Inglês e tradução para o Português disponíveis em:

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

[https://www.uschamber.com/sites/default/files/intl\\_nist\\_framework\\_portugese\\_finalfull\\_web.pdf](https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf)



# Todos Tem um Papel na Segurança e Proteção de Dados: Ecossistema é Complexo e Interdependente



# Obrigada

✉ cristine@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)

# Referências Adicionais sobre a Dinâmica de Trabalho e Maturidade dos CSIRTs

cert.br nic.br egi.br

# Tratamento de Incidentes: Pessoas e Relações de Confiança Fazem a Diferença

## **Incidentes não acontecem no vácuo**

- envolvem múltiplas organizações, redes e países
- resolução requer análise de informações internas e externas

## **CSIRTs operam em um esquema de governança em rede**

- não há hierarquia
- há a construção de redes de confiança globais e locais

## **Diversas Comunidades formadas ao redor do Globo**

- FIRST
- TF-CSIRT
- APCERT
- AfricaCERT
- NatCSIRTs
- EU e-CSIRT Network
- LAC-CSIRTs
- OIC-CERT

## **Maturidade evoluiu para um código de ética e modelos de acreditação e certificação**

- SIM3
- EthicsFIRST
- TF-CSIRT Trusted Introducer



# O que é um CSIRT

*A CSIRT is an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission.*

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

## Questões chave para o sucesso de um CSIRT

- Criar relações de confiança
- Ter uma rede de contatos
  - especialistas e outros CSIRTs
- Criar um ambiente favorável à notificação
  - sem caráter punitivo
  - sem possibilidade de impacto de auditoria

# O que um CSIRT não é

- Vítima
- Atacante
- Auditor
- Investigador
- Regulador
- Polícia

## Características de uma notificação de incidente

- Informal
- Foco é pedir ajuda
- Requer análise técnica para verificar
  - se é mesmo incidente
  - qual a natureza do incidente
  - qual o escopo

# Gestão de Incidentes: Processos

## Preparação da organização

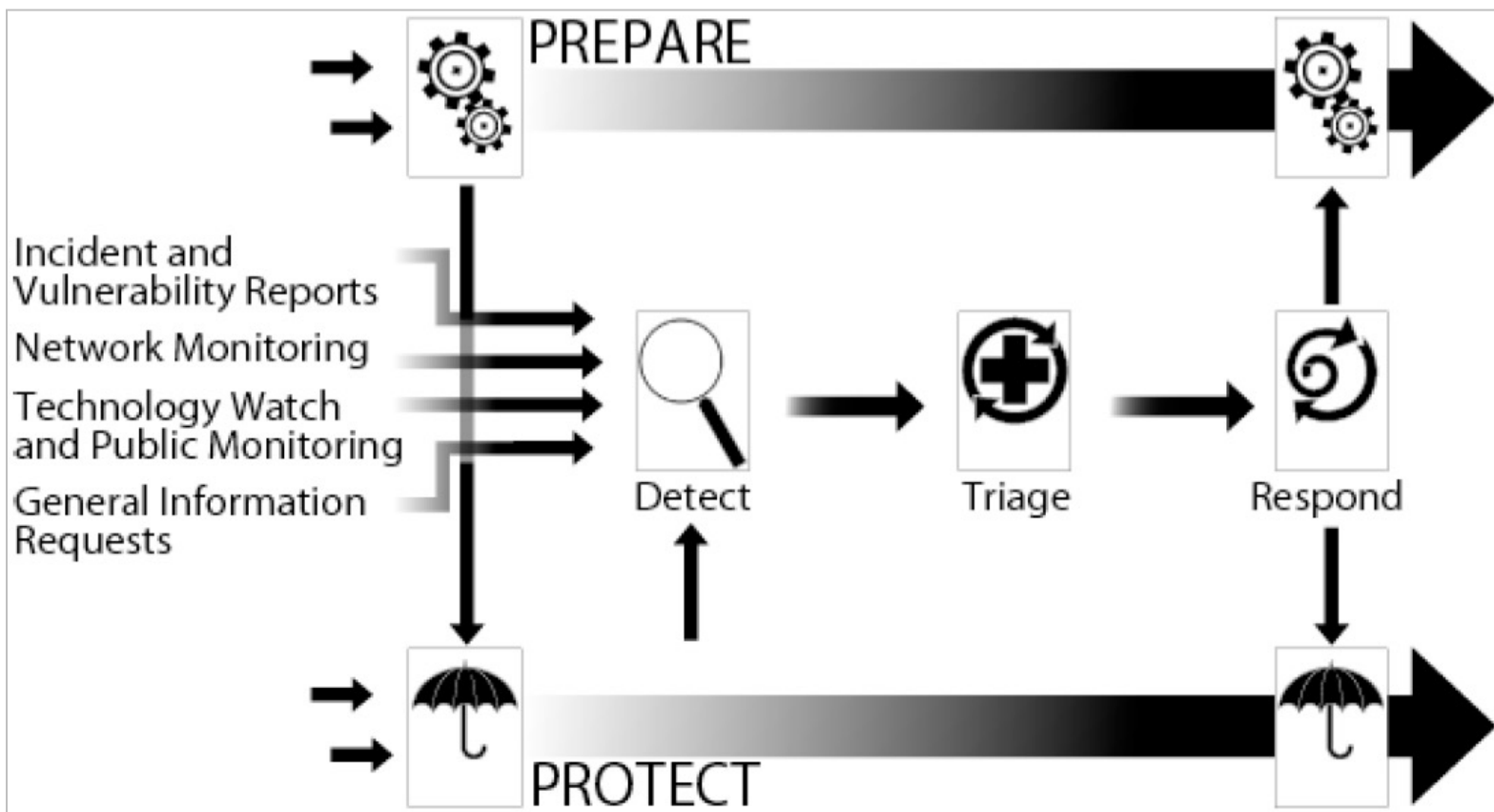
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT

## 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>

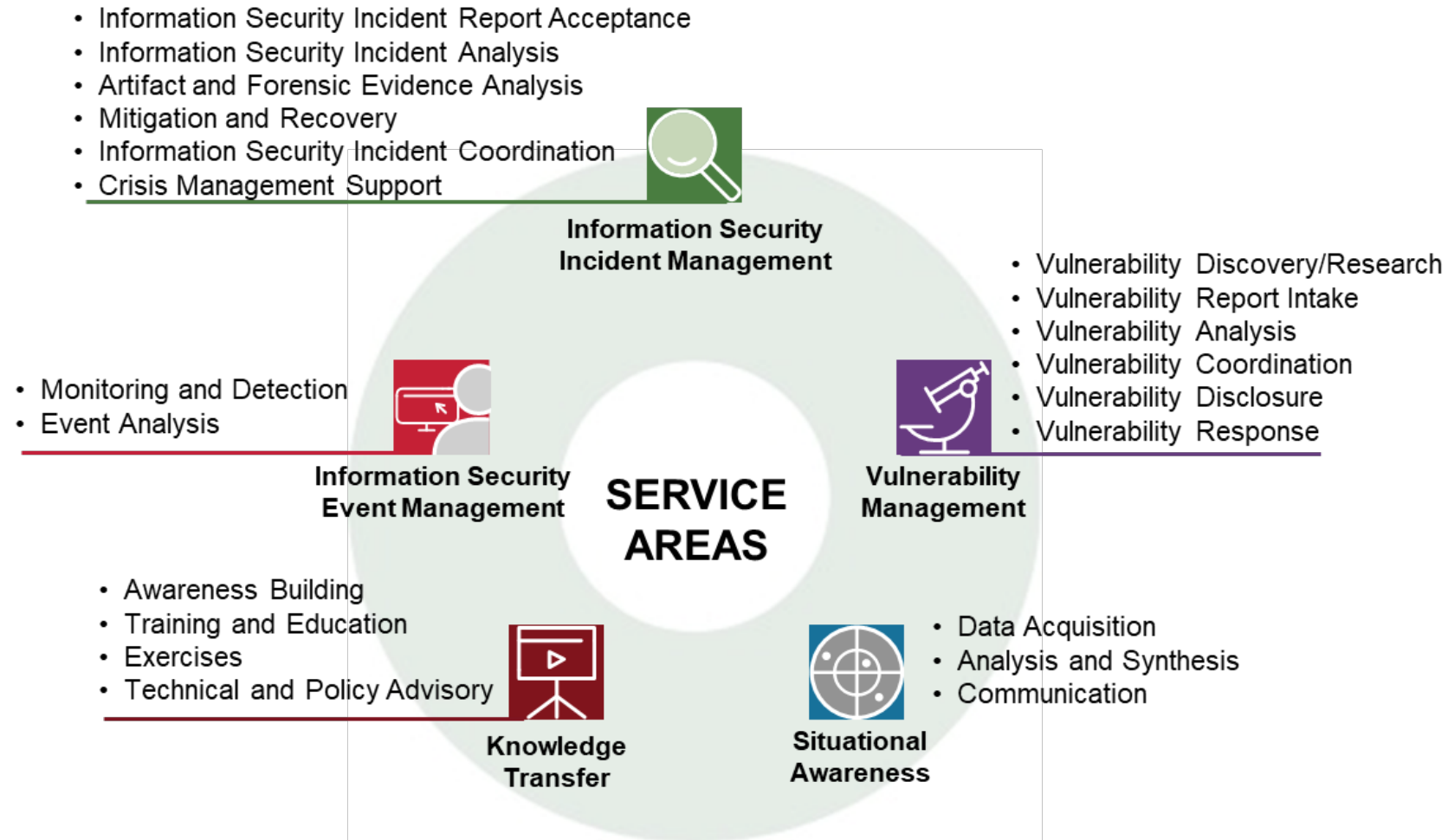
# FIRST CSIRT Services Framework: Estabelecimento e Melhoria Contínuas da Gestão de Incidentes

*“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/>

# FIRST CSIRT Services Framework: Estrutura, Autores e Próximos passos

## Estrutura

### Formato de cada área

- *Service Area*
- *Service*
  - *Function*
    - *Sub-Function*

## Próximos passos

- matriz de competências
- material de treinamento

## Autores

### Editor

- Klaus-Peter Kossakowski, Hamburg  
University of Applied Science

### Coordenadores de área

- Olivier Caleff, OpenCSIRT Foundation (FR)
- **Cristine Hoepers, CERT.br/NIC.br (BR)**
- Amanda Mullens, CISCO (US)
- Samuel Perl, CERT/CC (US)
- Daniel Roethlisberger, Swisscom (CH)
- Robin M. Ruefle, CERT/CC (US)
- Mark Zajicek, CERT/CC (US)

## Contribuidores

- Vilius Benetis, NRD CIRT (LT)
- Angela Horneman, CERT/CC (US)
- Allen Householder, CERT/CC (US)
- Art Manion, CERT/CC (US)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)



# FIRST CSIRT Services Framework: Overview of all CSIRT Services and related Functions



## SERVICE AREA Information Security Event Management

### Monitoring and Detection

- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

### Event Analysis

- Correlation
- Qualification



## SERVICE AREA Information Security Incident Management

### Information Security Incident Report Acceptance

- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

### Information Security Incident Analysis

- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

### Artifact and Forensic Evidence Analysis

- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

### Mitigation and Recovery

- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

### Information Security Incident Coordination

- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

### Crisis Management Support

- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication



## SERVICE AREA Vulnerability Management

### Vulnerability Discovery/Research

- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

### Vulnerability Report Intake

- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

### Vulnerability Analysis

- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

### Vulnerability Coordination

- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

### Vulnerability Disclosure

- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

### Vulnerability Response

- Vulnerability Detection/Scanning
- Vulnerability Remediation



## SERVICE AREA Situational Awareness

### Data Acquisition

- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

### Analysis and Synthesize

- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

### Communication

- Internal and External Communication
- Reporting and Recommendations
- Implementation



## SERVICE AREA Knowledge Transfer

### Awareness Building

- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

### Training and Education

- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

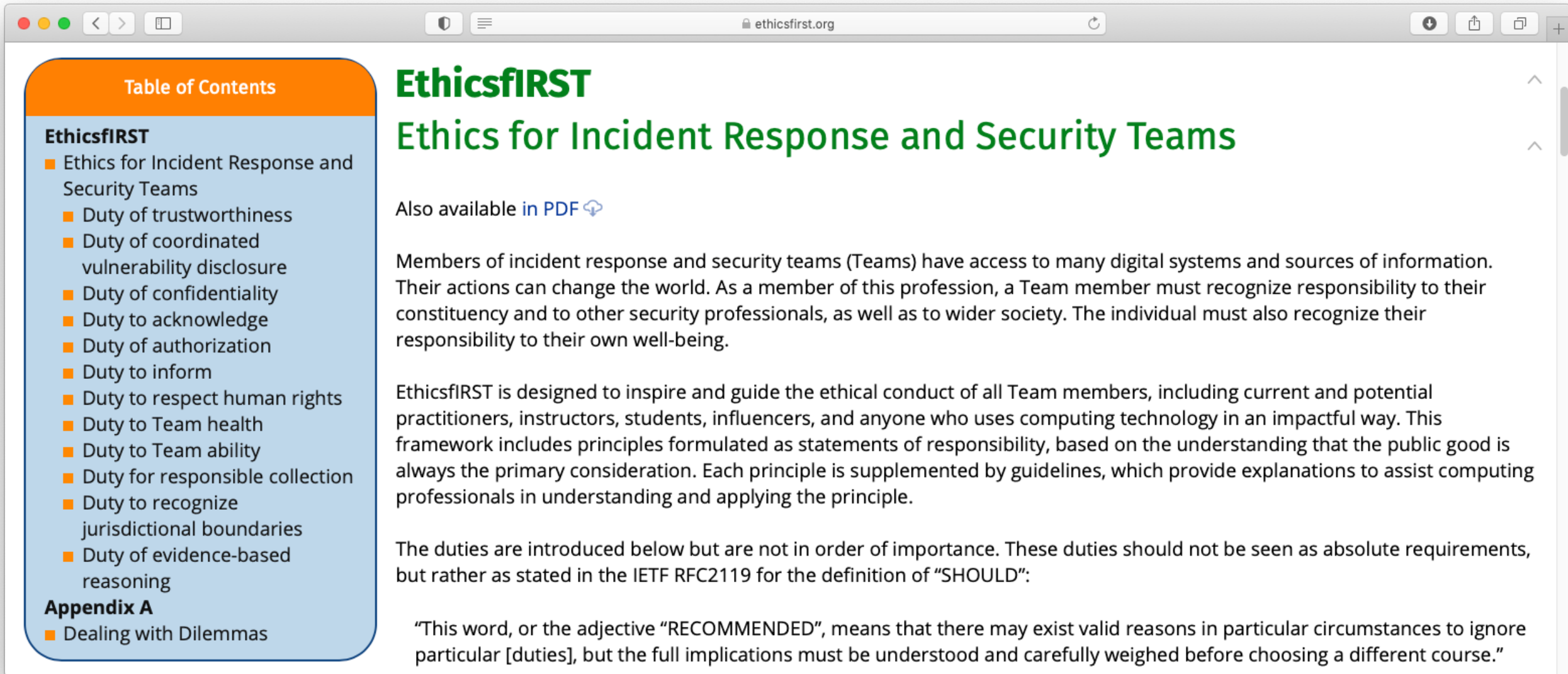
### Exercises

- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

### Technical and Policy Advisory

- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

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



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."

# 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)

## Como usar

- Cada comunidade escolhe os níveis de maturidade para seu contexto
- Os parâmetros são o ponto em comum

## 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 mXVIIIb<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 Drex, 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 mXVIII, 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 mXVIIIb 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/>

The screenshot displays the SIM3 Self Assessment Tool interface. The top navigation bar includes the Open CSIRT Foundation logo and the title 'SIM3 Self Assessment Tool'. 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. A radar chart on the right shows the assessment results for 'TI Certification not reached'.

**Organisation** **Human** Tools Processes

With **Humans** we refer to the people working together to provide the services described in the Organisation area and satisfy the mandate. All people contributing to the goals of the (CSIRT) organisation that manages security incidents, require a technical and/or management oriented education with considerable on-the-job training plus additional training for more detailed expertise like malware analysis or forensics. The 'H' parameters in this area are about the factors of importance in regard the most important factor in any CSIRT: the human 'capital' of the people working there.

Expand all / Collapse all

**H-1: Code of Conduct/Practice/Ethics**

Does your CSIRT provide guidance, guidelines or sets of rules for its team members on how to behave professionally, in an ethical manner? Often called a 'Code of Conduct (CoC)' or a 'Code of Practice (CoP)', it can provide golden rules on confidentiality, trustworthiness, and other key human qualities expected from CSIRT team members. The CSIRT's host organisation will often have an ethics code, but such codes are of a generic nature and have nothing to do with the specific work that the CSIRT does. The CSIRT often deals with highly sensitive data, and communicates not just inside the host organisation, but also outside. Also, responsible behaviour of CSIRT team members is not limited to the work context, but also relevant in private circles where security is concerned. The Trusted Introducer CCoP can be used as CoP baseline, as it was written specifically for CSIRTs. Alignment with the security policy (O-11) is necessary. Does your team support such a code of conduct/practice/ethics?

- 0 We never really discussed this.
- 1 We know what kind of work ethics are expected of us, but they were never written down.
- 2 We don't have a formal written code of conduct, therefore we wrote something for our own purposes. Our management has not formally approved this.
- 3 We have a written code of conduct approved by our team management.
- 4 We have a written code of conduct approved by our team management. In the periodic review of our team it is checked if and how this code has been used and if it serves its purpose.

**H-2: Personnel Resilience**

Does your CSIRT have enough staffing to deal with planned or unexpected team members' unavailability? Such cases include illness, holidays, quitting of job ... Depending on the services offered (O-5) and the service levels (O-7), the number of team members will vary, but ensuring

**Your SIM3 Assessment URL**

Please bookmark your results to start next time with this status:  
<https://sim3-check.opencsirt.org/#/v1/6waL3v2nV-5bNcAAe3X-Eo63PcQ6>

Choose your desired SIM3 Profile:

ENISA/GCMF Basic ENISA/GCMF Intermediate ENISA/GCMF Advanced **TI Certification**

Spider-Chart/Show questions Table of Results Open Actions [7]

If you click on a specific tile you will be directed to the associated parameter on the left side.