

nic.br egi.br

cert.br

Curso TCU / NIC.br
09 de junho de 2022
Evento Online

Aspectos Técnicos e Regulatórios sobre Internet

Aula 5: Segurança Cibernética

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

cert.br nic.br egi.br

Agenda

- Cenário atual e causas mais comuns dos incidentes
- Conceitos
 - ameaças, vulnerabilidades e riscos
 - segurança da informação
- Ecossistema de segurança cibernética
- *Frameworks* de segurança cibernética e gestão de incidentes
 - definições: incidente, CSIRT, gestão, tratamento e resposta a incidentes
 - *frameworks* mais adotados
- Gestão de incidentes no contexto da LGPD
- CSIRTs no Brasil
- Iniciativas por uma internet mais resiliente

Cenário Atual

cert.br nic.br egi.br

internationalIT

HOME SOLUÇÕES SERVIÇOS BLOG CONTATO

Brasil terá maior exercício de defesa cibernética do hemisfério sul

O Exercício Guardião Cibernético 3.0 é coordenado pelo Comando de Defesa Cibernética (ComDCiber) e faz parte da estratégia nacional de segurança do país. O [SENAI](#), a [Cisco](#) e a [RustCon](#) vão apoiar o treinamento de cibersegurança para 350 pessoas de 58 organizações públicas e privadas que será realizado pelo [Ministério da Defesa](#).

BANCO CENTRAL DO BRASIL

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro

Governo Digital

Estratégia Nacional de Segurança Cibernética

Publicado em 11/08/2021 15h13 | Atualizado em 12/08/2021 14h30

A **Estratégia Nacional de Segurança Cibernética - E-Ciber** é um conjunto de ações estratégicas do governo federal relacionadas a área de segurança cibernética até 2023. Corresponde ao primeiro módulo da [Estratégia Nacional de Segurança da Informação](#) estabelecendo ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto.

“ A E-Ciber orienta a sociedade brasileira sobre as principais ações do governo federal, em termos nacionais e internacionais, na área da

Agência Nacional de Telecomunicações

Anatel aprova Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações

Normativo entrará em vigor em janeiro de 2021 e prestadoras terão 180 para se adaptarem

Publicado em 17/12/2020 19h17 | Atualizado em 18/12/2020 11h20



Optiv Cybersecurity Technology Map

Navigate Cybersecurity at Optiv.com



Navigating the Security Landscape
 So much technology. So many vendors. Who does what?
<https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers>

DC police surveillance cameras were infected with ransomware before inauguration

Malware seized 70 percent of DC police DVRs a week before Trump's inauguration.

SEAN GALLAGHER - 1/30/2017, 5:12 PM



system just one week before Inauguration Day. *The Washington Post* reports that 70 percent of the DVR systems used by the surveillance network were infected with ransomware, rendering them inoperable for four days and crippling the city's ability to monitor public spaces.

<https://arstechnica.com/security/2017/01/dc-police-surveillance-cameras-were-infected-with-ransomware-before-inauguration/>

<https://www.wired.com/story/police-body-camera-vulnerabilities/>

The screenshot shows a Wired article page. At the top, the Wired logo is visible along with navigation links for Business, Culture, Gear, and More. The article is by Lily Hay Newman, dated 08.11.2018 03:00 PM, and is categorized under Security. The main headline is 'Police Bodycams Can Be Hacked to Doctor Footage'. Below the headline is a sub-headline: 'Analysis of five body camera models marketed to police departments details vulnerabilities could let a hacker manipulate footage.' A video player is embedded in the article, showing a person's hands holding a body camera. The video title is 'Hacking Police Body Cameras' and it includes a subtitle 'used by law enforcement across the United States'. The video player shows a progress bar at 0:05/5:18. At the bottom of the page, there is a promotional banner for '3 FREE ARTICLES LEFT THIS MONTH' with a 'Subscribe' button.

olhardigital.com.br

MENU **OLHAR DIGITAL** 🔍

STJ se restabelece após ransomware; PF investiga cópia de dados

Renato Santino | 13/11/2020 21h45, atualizada em 13/11/2020 21h50

infomoney.com.br

InfoMoney

O "lado B" da digitalização

Fleury é o mais recente episódio de ransomware; veja como os ataques cibernéticos têm afetado os mercados

Vistos como algumas das maiores ameaças da era atual, sequestros de dados, ou ransomware, viram novo risco a ser monitorado no mercado

www1.folha.uol.com.br

JBS pagou US\$ 11 mi em resposta a ataque ransomware em operações na América do Norte

Empresa cancelou turnos em fábricas nos EUA e Canadá na semana passada, após ser afetada por ciberataque

9.jun.2021 às 21h26

🔊 Ouvir o texto A- A+

REUTERS A JBS USA, subsidiária da brasileira JBS nos Estados Unidos, confirmou em comunicado divulgado nesta quarta-feira (9) que pagou o equivalente a US\$ 11 milhões (R\$ 55,5 milhões) em resposta [a um ataque hacker](#) contra suas operações

poder360.com.br

PODER 360 | Diretor Fernando Rodrigues

Renner diz não ter pago resgate de dados depois de ataque hacker

A varejista sofreu uma invasão na última 5ª feira (19.ago.2021), mas informou que principais bancos de dados estão preservados

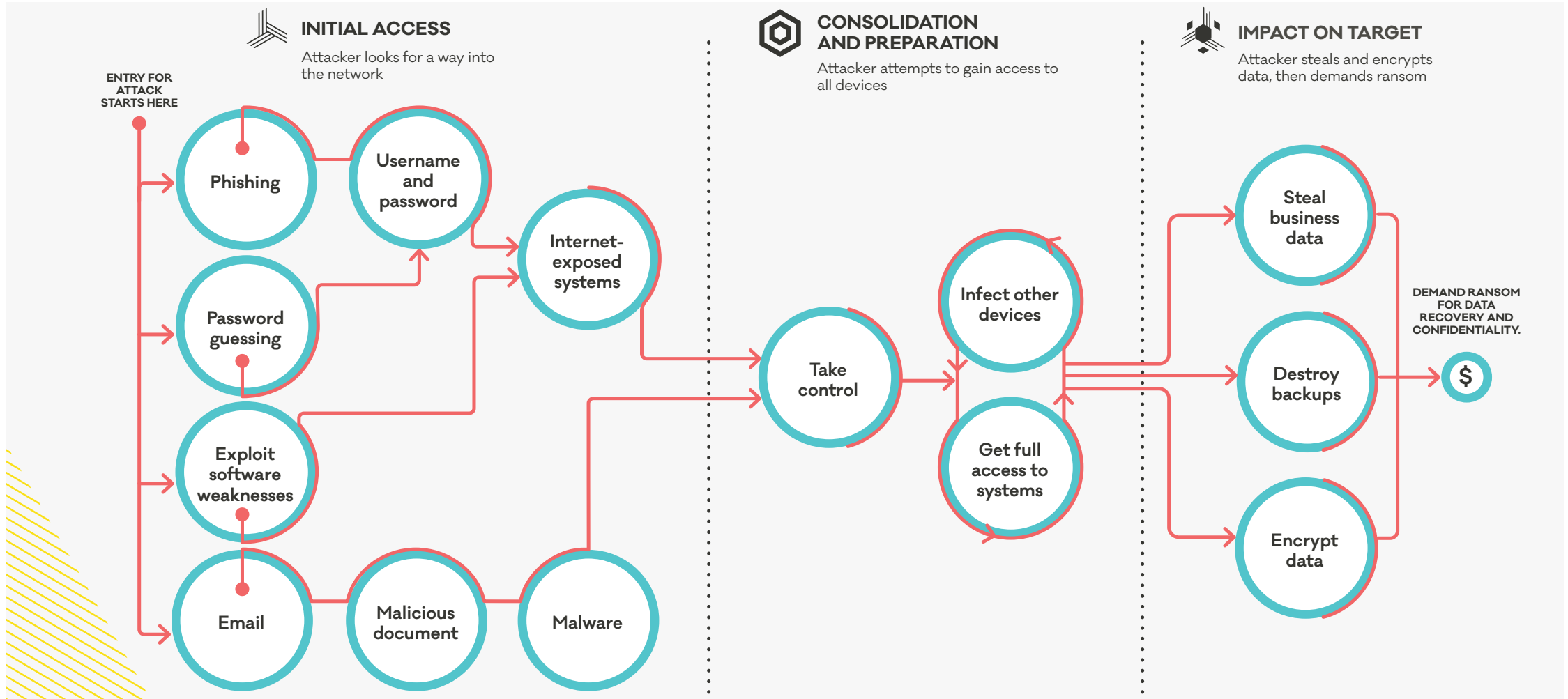
Compartilhe

📄 🐦 🗨️ 📍 +



Divulgação/Renner

Diagnóstico da Microsoft sobre o sucesso dos *ransomwares*: **CERT NZ How Ransomware Works**




<https://www.cert.govt.nz/business/guides/protecting-from-ransomware/>

<https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware>

Menu Search **Bloomberg** Sign In **Subscribe**

Bloomberg **Cybersecurity**



Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By [William Turton](#) and [Kartikay Mehrotra](#)
June 4, 2021, 4:58 PM GMT-3

- ▶ Investigators suspect hackers got password from dark web leak
- ▶ Colonial CEO hopes U.S. goes after criminal hackers abroad

<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

SolarWinds – Ataque atribuído à Rússia pelos EUA

Causas: senha vazada + exploração de vulnerabilidades

SolarWinds FTP credentials were leaking on GitHub

in November 2019 Featured

3

Shares



Share



Tweet

3

By **Sam Varghese**

More details are emerging about poor security at SolarWinds, following the compromise of its Orion network management software that was then used to effect attacks on many companies in a number of regions around the globe.

A researcher from India had advised SolarWinds in November 2019 that he had found a public GitHub repository which was leaking the company's FTP credentials.

Downloads Url: <http://downloads.solarwinds.com>
FTP Url: <ftp://solarwinds.upload.akamai.com>
Username:
Password:
POC: <http://downloads.solarwinds.com/test.txt>

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

bounty hunter, said in a tweet: "Was
raging SolarWinds. Hmmm, how that
d was *****123 Rolling on the floor

<https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html>

<https://threatpost.com/solarwinds-default-password-access-sales/162327/>

<https://us-cert.cisa.gov/remediating-apt-compromised-networks>

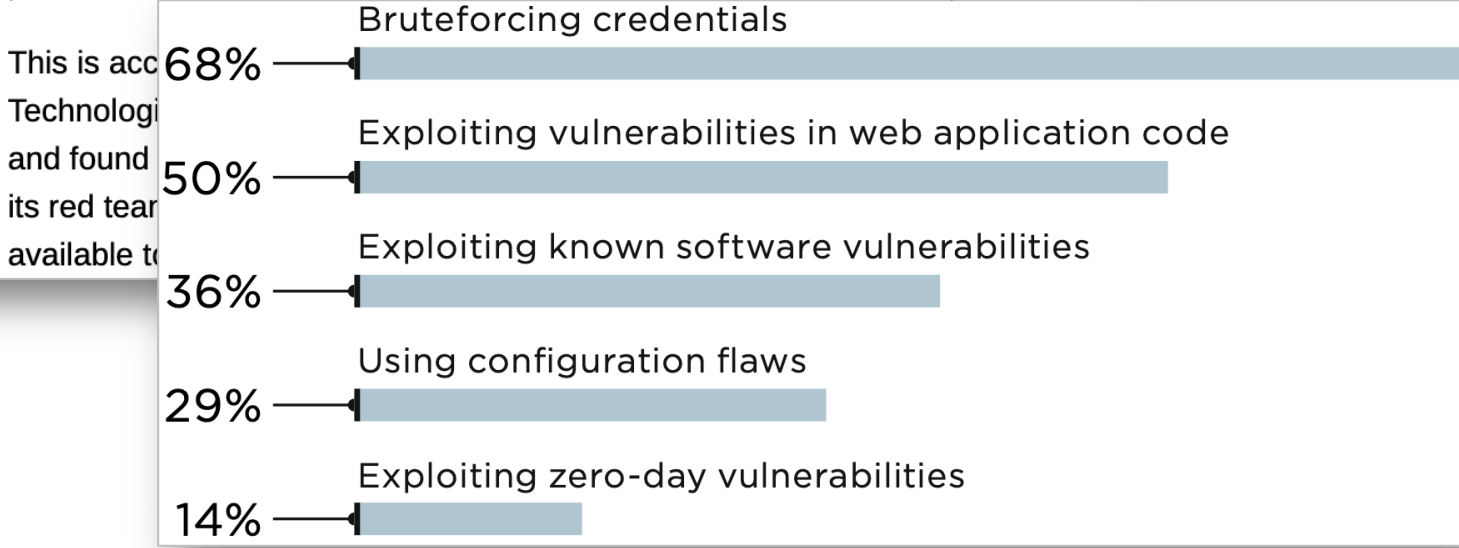
You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

Three little words: Patches, passwords, policies

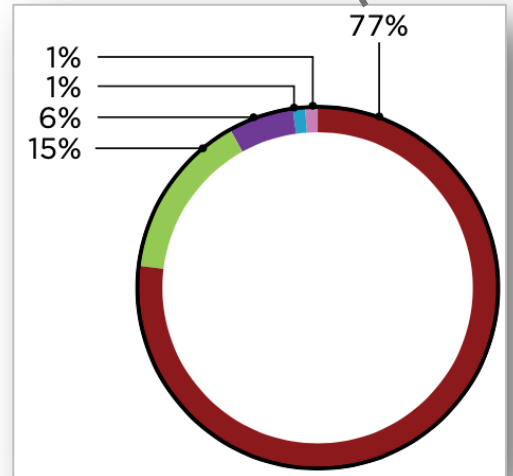
Thu 13 Aug 2020 // 07:06 UTC

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.



- 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



https://www.theregister.com/2020/08/13/pentest_networks_fail/
<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf>

Personal data of 16 million Brazilian COVID-19 patients exposed online

The personal and health information of more than 16 million Brazilian COVID-19 patients has been leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub this month.

Those affected by the leak are Brazil President Jair Bolsonaro, several ministers, and 17 provincial governors.



By Catalin Cimpanu for Zero Day | November 26, 2020 -- 21:22 GMT (13:22 PST) | Topic: Coronavirus: Business and technology in a pandemic

Data of 243 million Brazilians exposed online via website source code

The password to access a highly sensitive Ministry of Health database was stored inside a government site's source code.

Since a website's source code can be accessed and reviewed by anyone pressing F12 inside their browser, Estadao reporters searched for similar issues in other government sites.

Reporters said the site's source code contained a username and password stored in Base64, an encoding format that can be easily decoded to obtain the initial username and password, with little to no effort.



By Catalin Cimpanu for Zero Day | December 3, 2020 -- 14:17 GMT (06:17 PST) | Topic: Security

<https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/>
<https://www.zdnet.com/article/data-of-243-million-brazilians-exposed-online-via-website-source-code/>

Where leaks come from

- 01 India
- 02 Brazil
- 03 United States
- 04 Nigeria
- 05 France
- 06 Russia
- 07 UK
- 08 Canada
- 09 Bangladesh
- 10 Indonesia

Uber Data Breach*

May 2014

Hackers discovered credentials in a personal public repository on GitHub that granted access to a database containing private information of thousands of Uber drivers.

[*Read the article](#)

27.6%

Starbucks Data Breach*

January 2020

JumpCloud API key found in GitHub repository.

[*Read the article](#)

Equifax Data Breach*

April 2020

Leaked secrets in personal GitHub account granted access to sensitive data for Equifax customers.

[*Read the article](#)

UN Data Breach*

January 2021

.gitcredentials in a public repository giving hackers access to private repositories with sensitive information.

[*Read the article](#)

Google keys

Development tools

Django, RapidAPI, Okta

Data storage

MySQL, Mongo, Postgres...

Other

including CRM, cryptos, identity providers, payments systems, monitoring

Messaging systems

Discord, Sendgrid, Mailgun, Slack, Telegram, Twilio...

Cloud provider

AWS, Azure, Google, Tencent, Alibaba...

Private keys

15.9%

15.4%

12%

11.1%

8.4%

6.7%

State of Secrets Sprawl on GitHub - 2021: <https://blog.gitguardian.com/state-of-secrets-sprawl-2021/>

Intertrust Releases 2021 Report on Mobile Finance App Security

Report of over 150 mobile finance apps reveals a high level of security vulnerabilities across both iOS and Android, highlighting the importance of in-app security

June 02, 2021 12:00 PM Eastern Daylight Time

SAN FRANCISCO--(BUSINESS WIRE)--Intertrust, the pioneer in digital rights management (DRM) technology and leading provider of application security solutions, today released its [2021 State of Mobile Finance App Security Report](#). The report reveals that 77% of financial apps have at least

“Poor financial app security puts both financial organizations and their customers at risk, especially given the rise in cyberattacks over the course of the pandemic. This report shines a light on the ongoing threats and helps finance app vendors understand the importance of building in security mechanisms from day one”

 [Tweet this](#)

payment and customer data and putting the application code at risk for analysis and tampering.

One or more security flaws were found in every app tested

84% of Android apps and 70% of iOS apps have at least one critical or high severity vulnerability

81% of finance apps leak data

49% of payment apps are vulnerable to encryption key extraction

Banking apps contain more vulnerabilities than any other type of finance app

Cryptographic issues pose one of the most pervasive and serious threats, with 88% of analyzed apps failing one or more cryptographic tests. This means the encryption used in these financial apps can be easily broken by cybercriminals, potentially exposing confidential

<https://www.businesswire.com/news/home/20210602005213/en/Intertrust-Releases-2021-Report-on-Mobile-Finance-App-Security>

Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores do CERT.br:

- Acesso indevido via **senhas fracas** ou **comprometidas/vazadas**
 - 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

Veja também: 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

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

Barreiras: formação dos profissionais e priorização por gestores

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/>

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

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)**

Segurança da Informação e Segurança Cibernética

cert.br nic.br egi.br

Algumas Definições: Ameaças, Vulnerabilidades e Riscos

Riscos:

- indisponibilidade de serviços
- vazamento ou perda de dados
- perda de privacidade
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Ativos
(Sistemas, Dados e Pessoas)



Opções para lidar com o risco:

Aceitar

Transferir

- ex: seguro

Eliminar

- remover um dos vértices

Mitigar (gestão de risco)

- única real opção

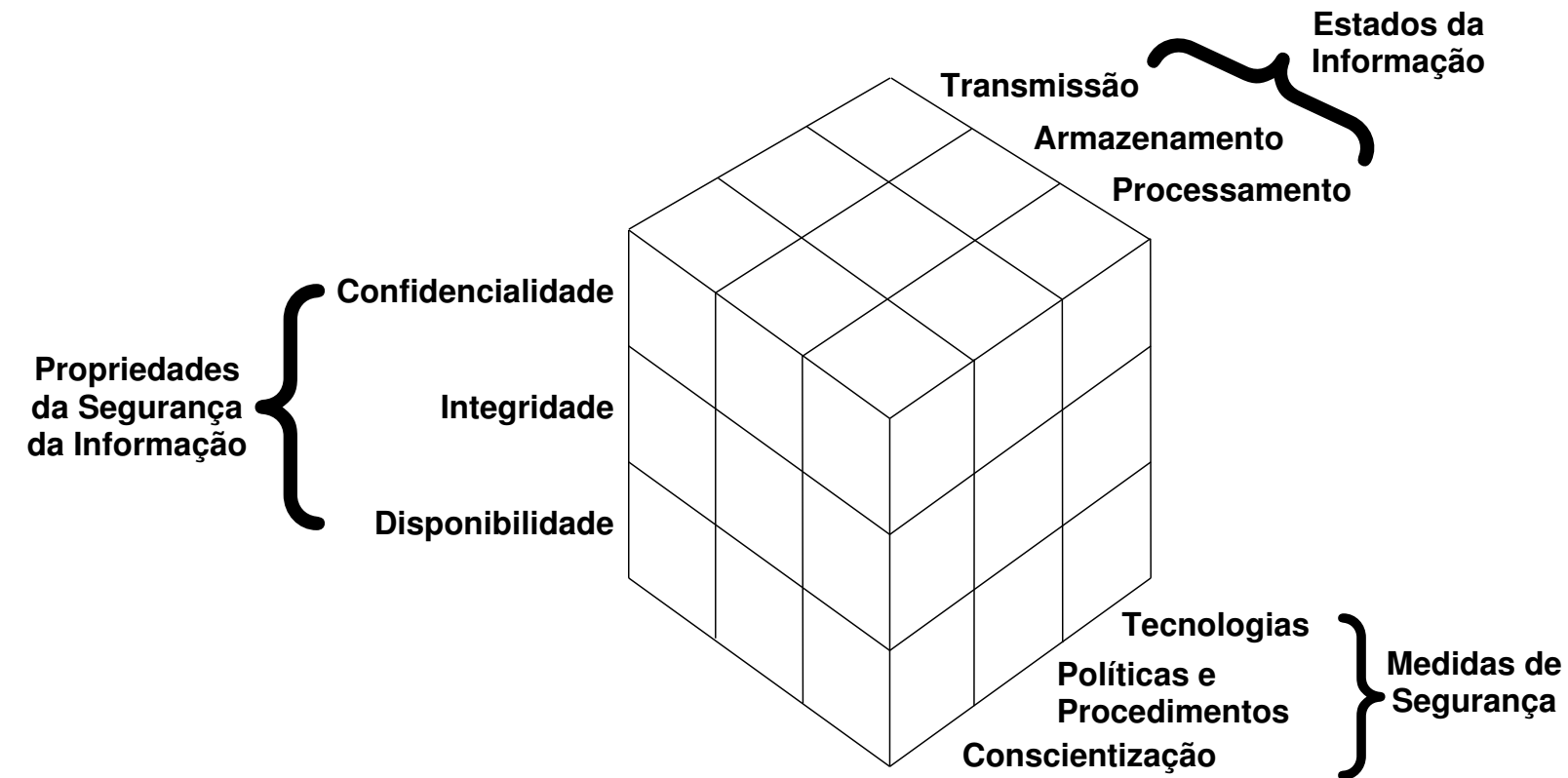
Ameaças

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

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

Segurança da Informação: É um Processo Complexo



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**

McCumber Information Security Model

<http://www.ibm.com/developerworks/security/library/s-confnotes2/>

Propriedades da Segurança da Informação

Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

Privacidade vs. Confidencialidade

Do ponto de vista de Segurança da Informação:

Privacidade – habilidade e/ou direito de proteger suas informações pessoais, estende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.

Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.



Fonte: *Security Engineering, 2nd Edition*, 2008, Ross Anderson

<http://www.cl.cam.ac.uk/~rja14/book.html>

Importância da Criptografia

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais (ex: atualização de *software* depende de assinaturas)
- mecanismos de autenticação (ex: acesso a contas de *e-mail* e redes sociais)
- conexão segura na Web (HTTPS)
 - confidencialidade
 - integridade (Estou conectando no *site* que eu realmente queria? O conteúdo não foi alterado no meio do caminho?)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC) e segurança de roteamento (RPKI)
- *blockchain*

Ecosistema de Segurança Cibernética

cert.br nic.br egi.br

Todos Tem um Papel na Segurança: Ecossistema é Complexo e Interdependente



Quase tudo é *software* e está conectado à Internet

Ataques são constantes

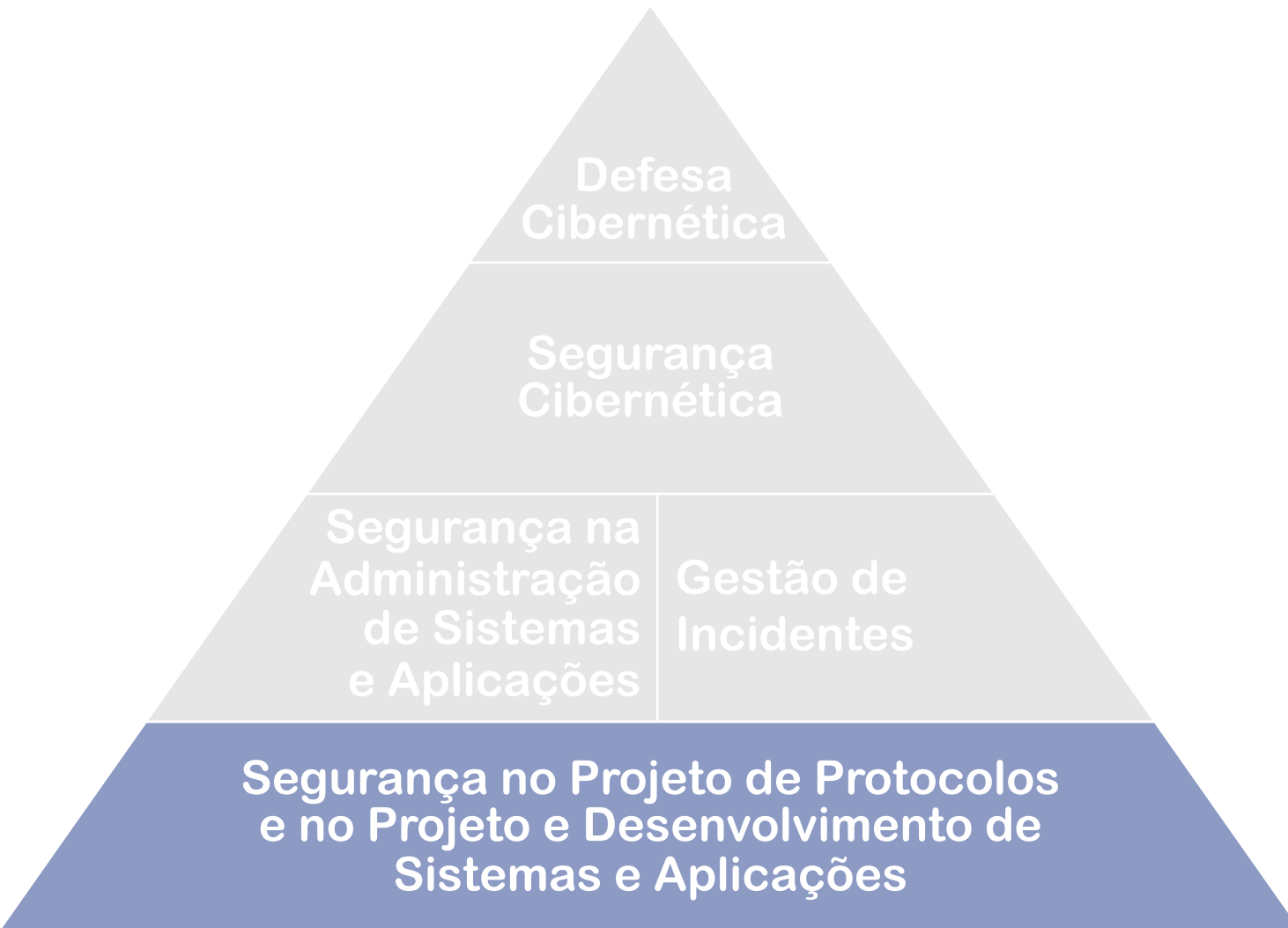
- Motivações diversas
- Volume crescente
 - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

O Desenvolvimento Precisa Ser Sólido para Reduzir a Superfície de Ataque



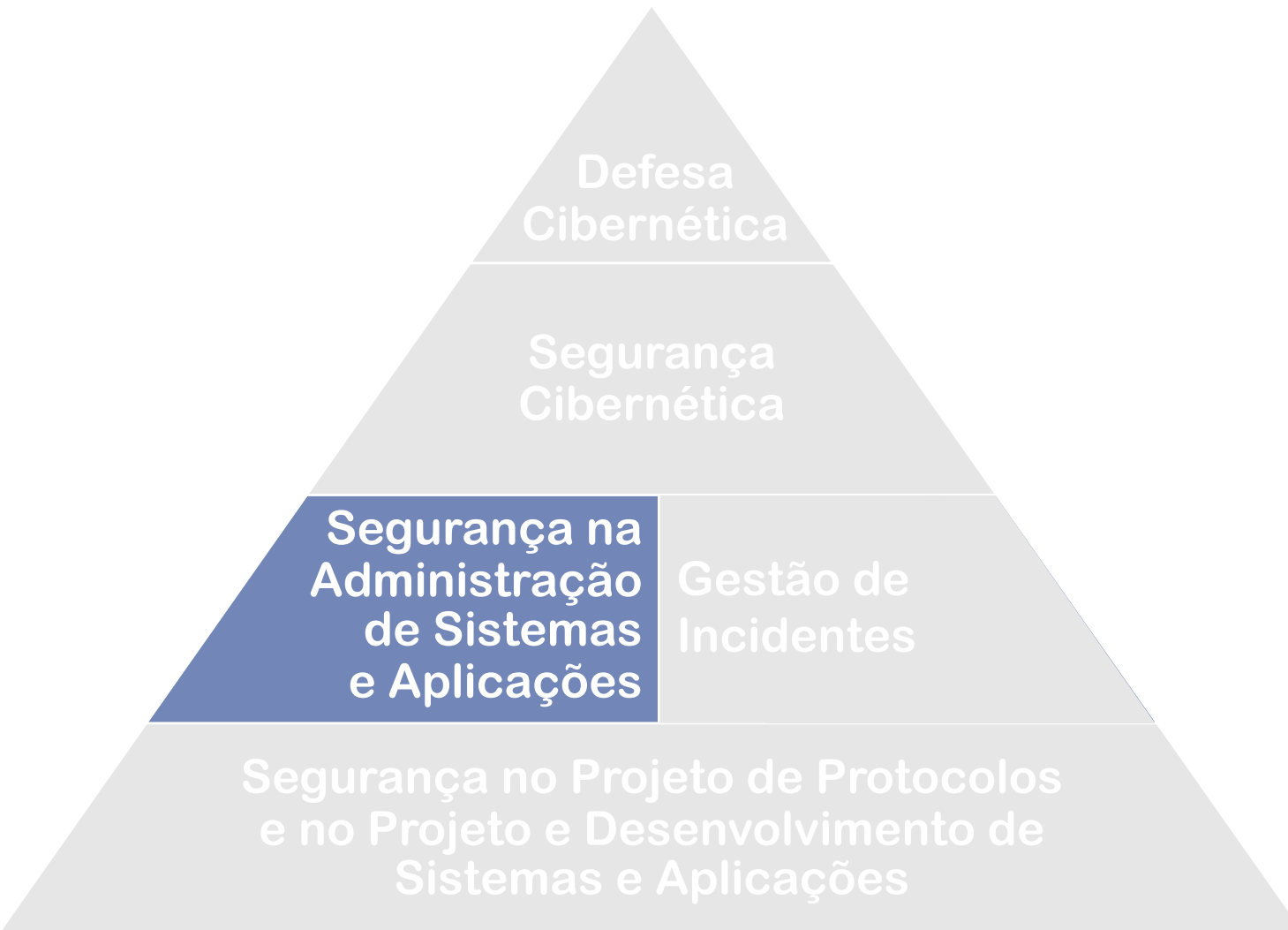
Postura dos desenvolvedores de *software* deve considerar segurança

- não se pode pensar “que alguém vai cuidar da segurança depois”

Atores chave para melhora da base

- Mercado e Governo: demanda por segurança e não só por funcionalidades
- Professores das áreas de Eng. de *Software* e Programação
 - MEC, Capes, CNPq, SBC, MCTIC
- Empresas de *Software* e *Hardware*
 - seguir requisitos mínimos de segurança
 - fugir de certificações de *software*

A Implantação das Tecnologias Precisa Focar em Boas Práticas de Segurança



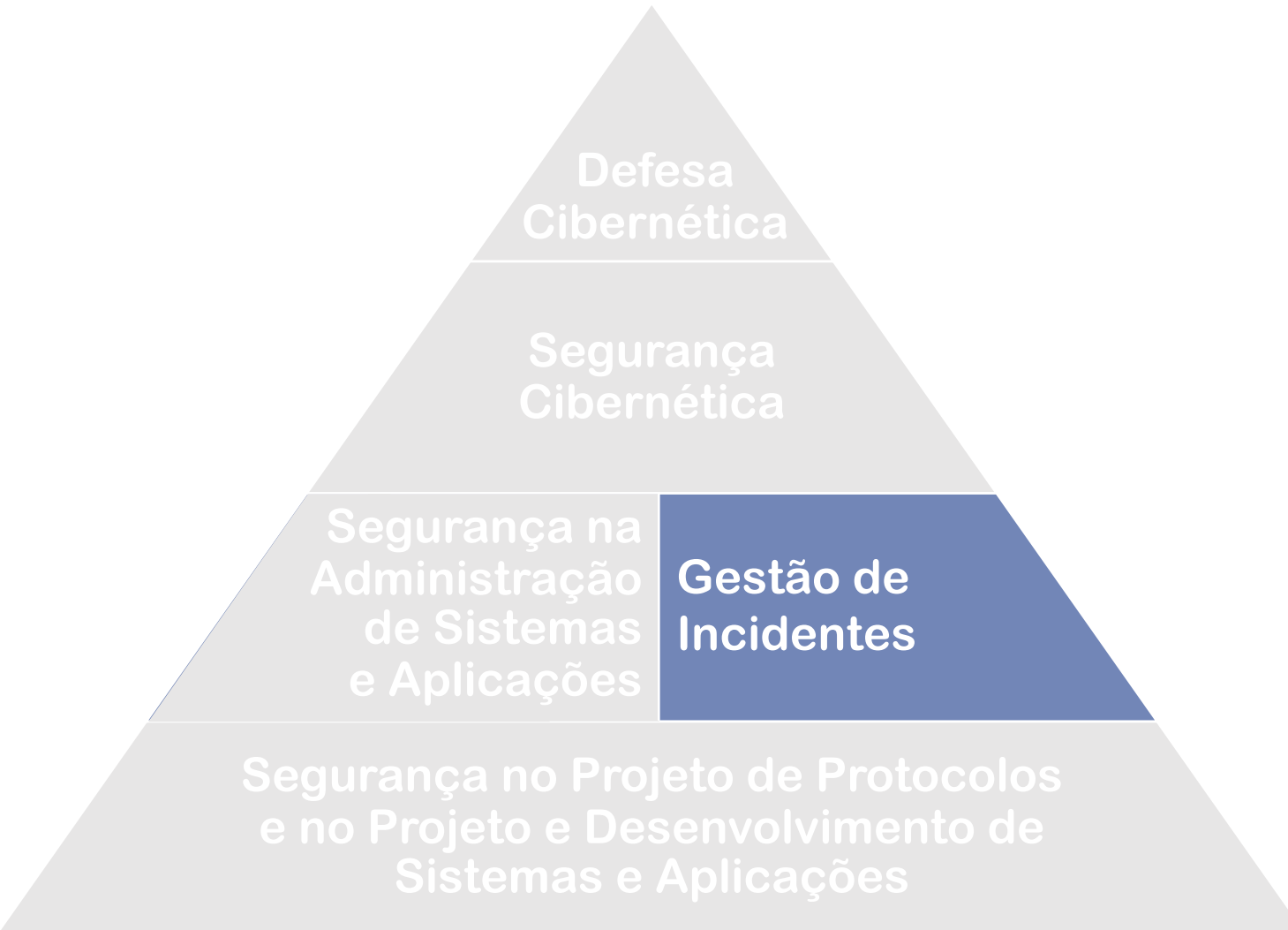
Desafios

- Sistemas com muitos problemas
 - vulnerabilidades
 - sem instrumentação para permitir configurações mais seguras
- Poucos profissionais com sólidos conhecimentos de Internet
- Complexidade dos ambientes

Necessário Seguir Padrões Abertos e Boas Práticas Globais

- Aumentam a segurança
- Mantém a interoperabilidade
 - essencial para inovação e desenvolvimento

O Tratamento Ágil e Adequado Reduz Danos e Vítimas



Incidentes ocorrerão

- Ataques novos todos os dias
- Complexidade dos ambientes dificulta proteção e detecção

Foco precisa ser em

- Aumentar os níveis de segurança e resiliência das redes
- Treinar profissionais na área
- Fomentar a criação de CSIRTs (Times de Tratamento de Incidentes) em todas as esferas
- Criar massa crítica para uma comunidade nacional ativa

Efetividade das Soluções e Ferramentas de Segurança Depende da Base Sólida



Segurança cibernética depende de

- Cooperação de todos os atores
- Sistemas menos vulneráveis
- Ambiente bem projetado para permitir uso adequado das ferramentas

Precisa ser um processo

- Com apoio político
- Que habilite as bases da pirâmide a implementarem o que for necessário
- Com envolvimento de todas as esferas
 - da alta gestão ao usuário

Atores chave para efetividade

- Governo: DSI/GSI (normas), Órgãos de Controle, Alta Gestão
- Empresas: Alta Gestão
- Academia: formação de qualidade

A Defesa Cibernética é um Nicho Especializado mas a Eficácia Dependerá das Ações de Todos os Atores



Nenhum grupo ou estrutura resolverá o problema sozinho

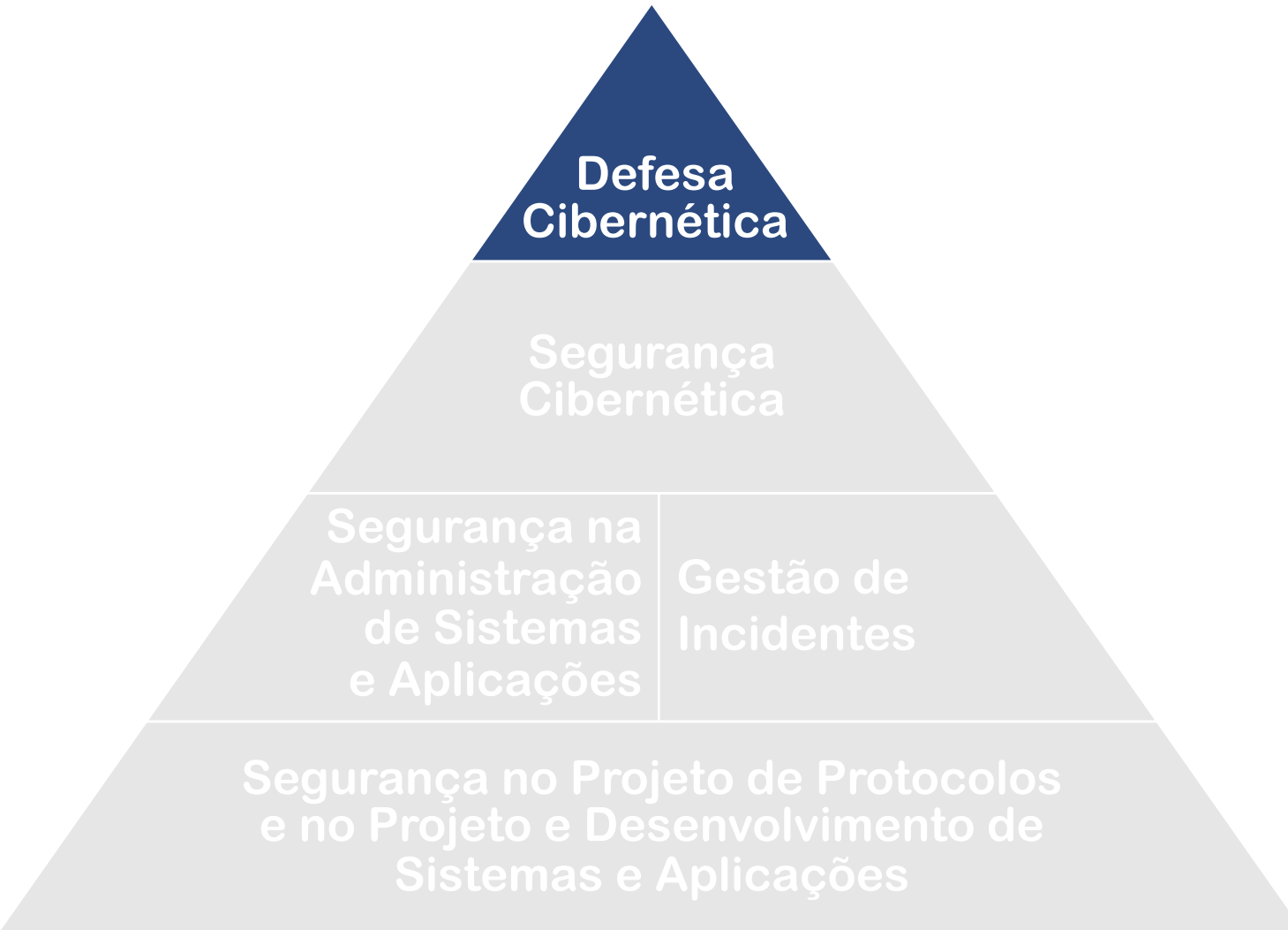
A segurança se faz nas “pontas”

- depende de *software* seguro
- depende de redes resilientes

As “pontas” não conseguem

- coletar inteligência sobre ataques vindos de outras nações
- dedicar recursos para estudar vetores de ataques de baixa probabilidade mas altíssimo impacto

Defesa Cibernética: Sistema Militar de Defesa Cibernética (SMDC)



O órgão central é o Comando de Defesa Cibernética (ComDCiber)

- comando operacional conjunto, permanentemente ativado e com capacidade interagências

A capacidade interagências caracteriza-se pela atuação colaborativa com representantes

- de órgãos da APF
- de infraestruturas críticas
- de outros órgãos, instituições e empresas, públicos ou privados, de interesse da Defesa.

[Portaria Nº 3.781/GM-MD, de 17 de novembro de 2020](#)
[Doutrina de Operações Conjuntas, MD30-M-01, Min. da Defesa](#)

Atuação do NIC.br e do Comitê Gestor da Internet no Brasil: Ajudar a Construir um Ecossistema Internet mais Saudável

**Princípios para a Governança e
Uso da Internet:**

**8. Funcionalidade, segurança e
estabilidade**

A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.



<https://principios.cgi.br/>

***Frameworks* de Segurança e Gestão de Incidentes**

cert.br nic.br egi.br

Primeiramente algumas definições:

Incidentes de Segurança e CSIRTs/CERTs

Incidente de Segurança em Computadores

- cada organização precisa consolidar em política a sua própria definição, em geral com base na missão, serviços e recursos disponíveis
- de maneira genérica inclui: eventos adversos, confirmados ou sob suspeita, relacionados à segurança dos sistemas de computação ou das redes de computadores

Exemplos:

- Tentativas de ataques: varreduras, tentativa de adivinhar senhas, tentativas de infecção por *malware*, etc
- Ataques com sucesso: invasões, infecção por *malware*, negação de serviço (DDoS), desfiguração de página (*defacement*), etc

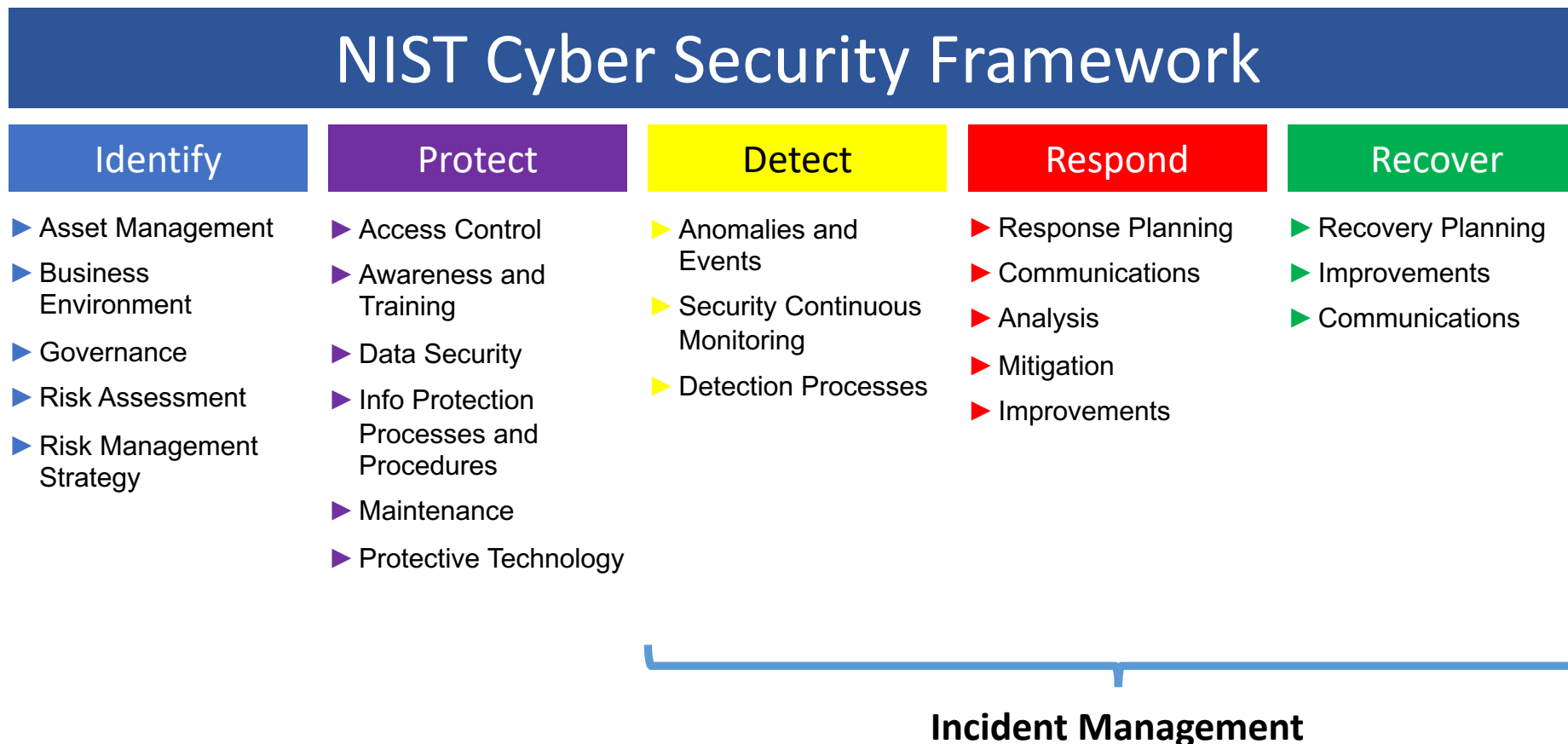
CSIRT(*)

Time de Resposta a Incidentes de Segurança

- acrônimo internacional para designar um time responsável por tratar incidentes de segurança para um público alvo específico
 - Outros acrônimos: IRT, CERT, CIRC, CIRT, SERT, SIRT
 - No Brasil também usados: ETIR, CTIR

* do Inglês “*Computer Security Incident Response Team*”

NIST Cyber Security Framework: Gestão de Riscos, Segurança e Gestão de Incidentes



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

SEI/CMU Incident Management Processes for CSIRTs: Gestão e Tratamento de Incidentes

Gestão de Incidentes – políticas e estratégias

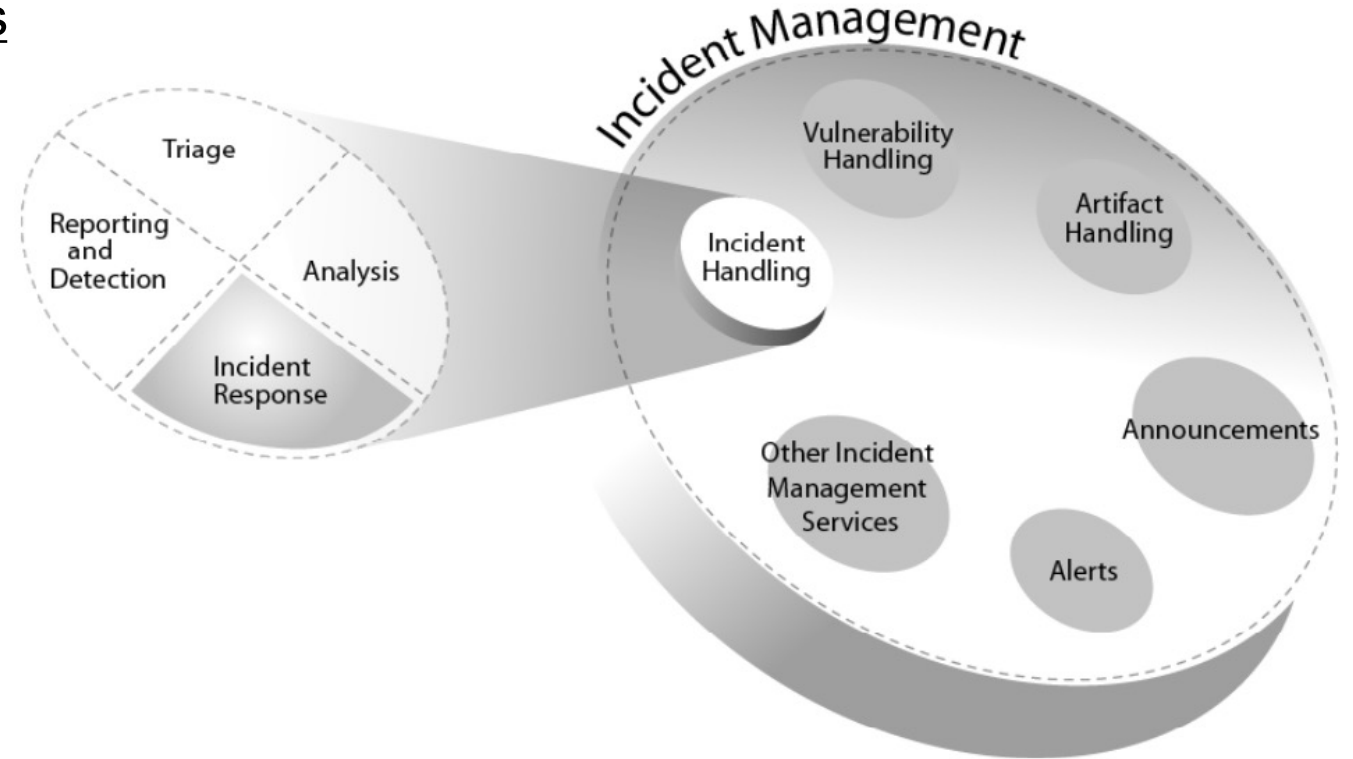
- gestão fim a fim de eventos e incidentes
- envolve toda a organização

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>

SEI/CMU Incident Management Processes for CSIRTs: Processos Complementares para Atingir Resiliência

Preparação da organização

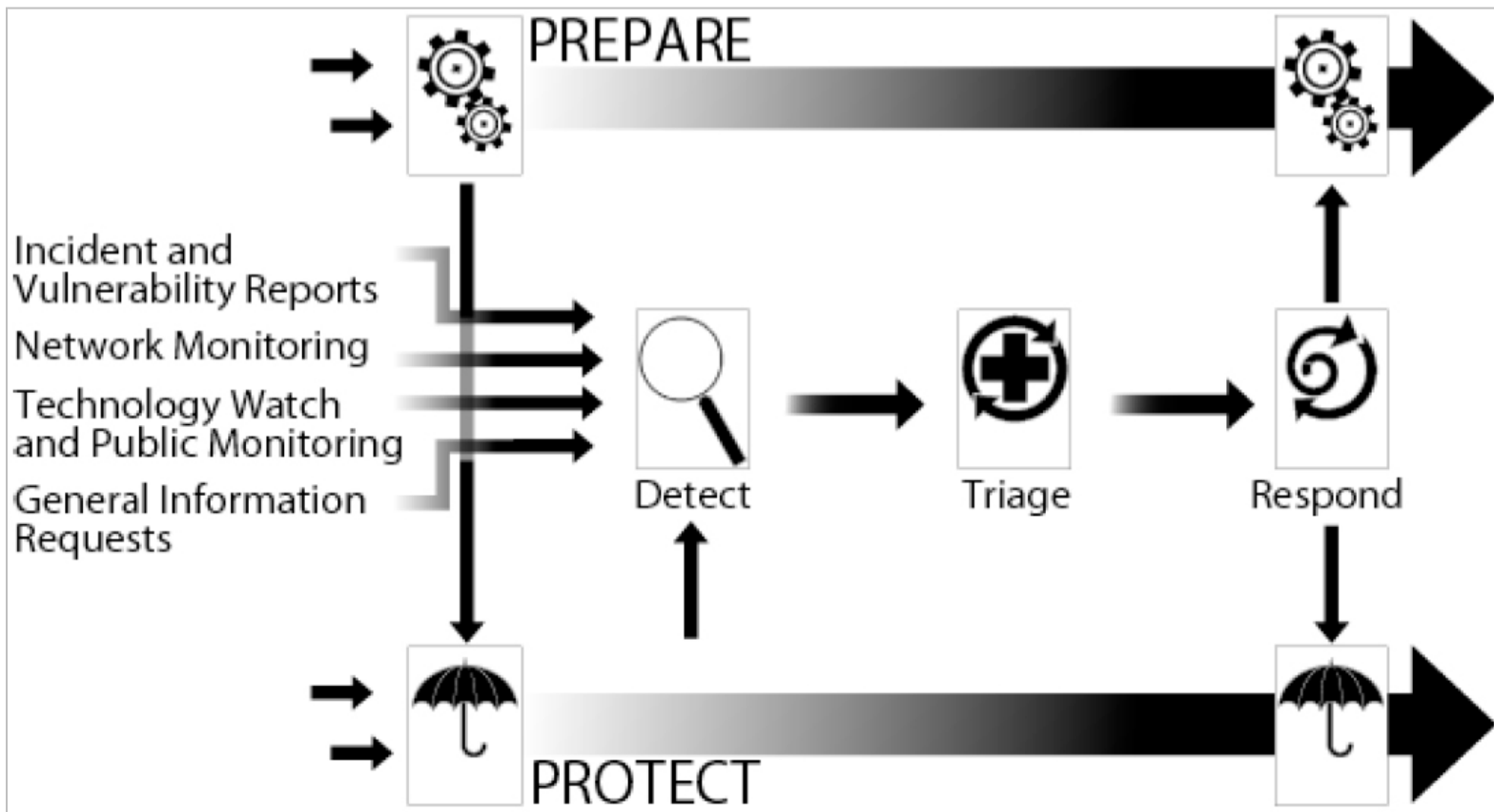
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas e processos
- planejar e implantar um CSIRT

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>

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 (relato) de incidente

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

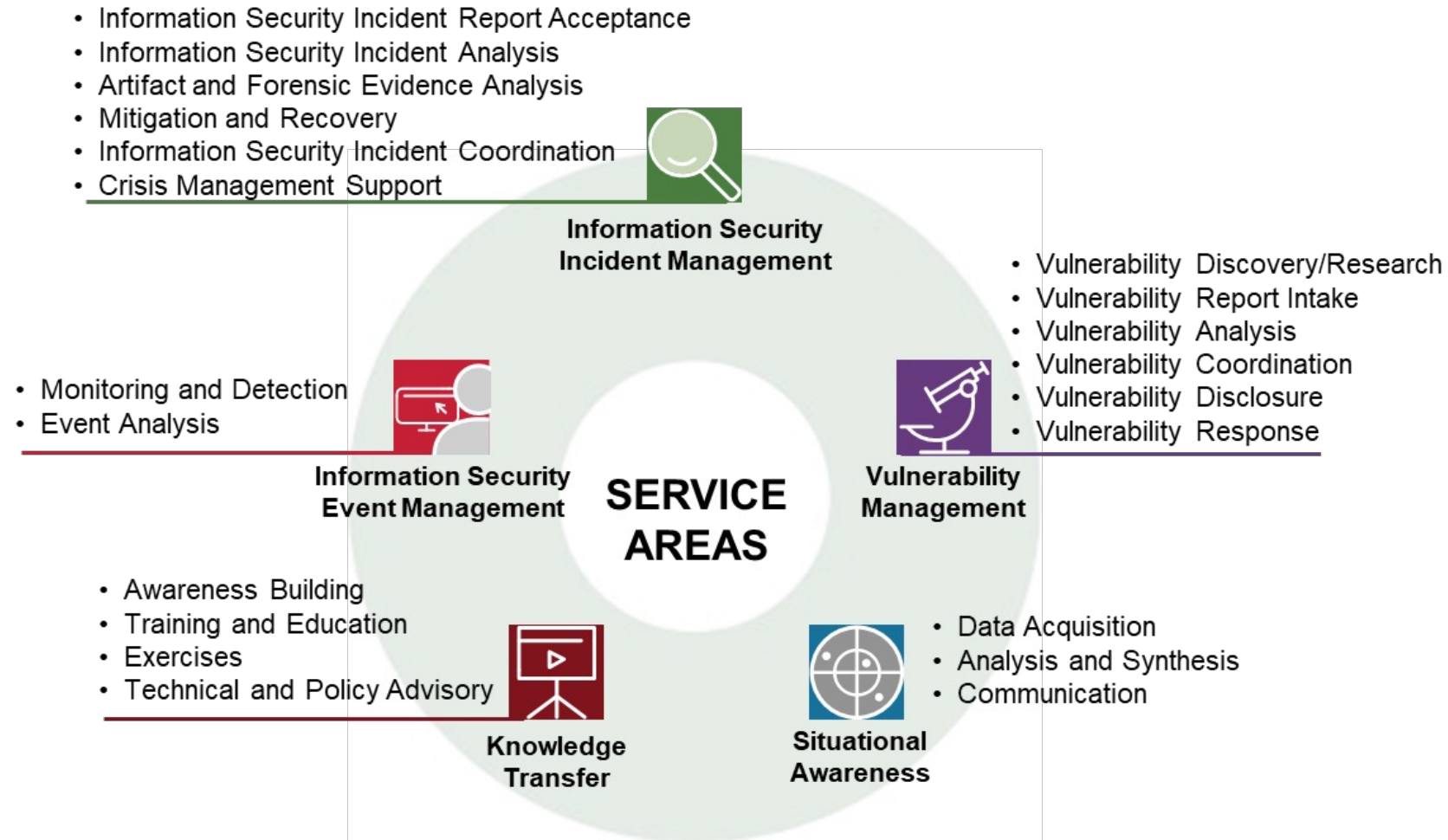
FIRST CSIRT Services Framework: Estabelecimento e Melhoria Contínuas da Gestão de Incidentes

“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*

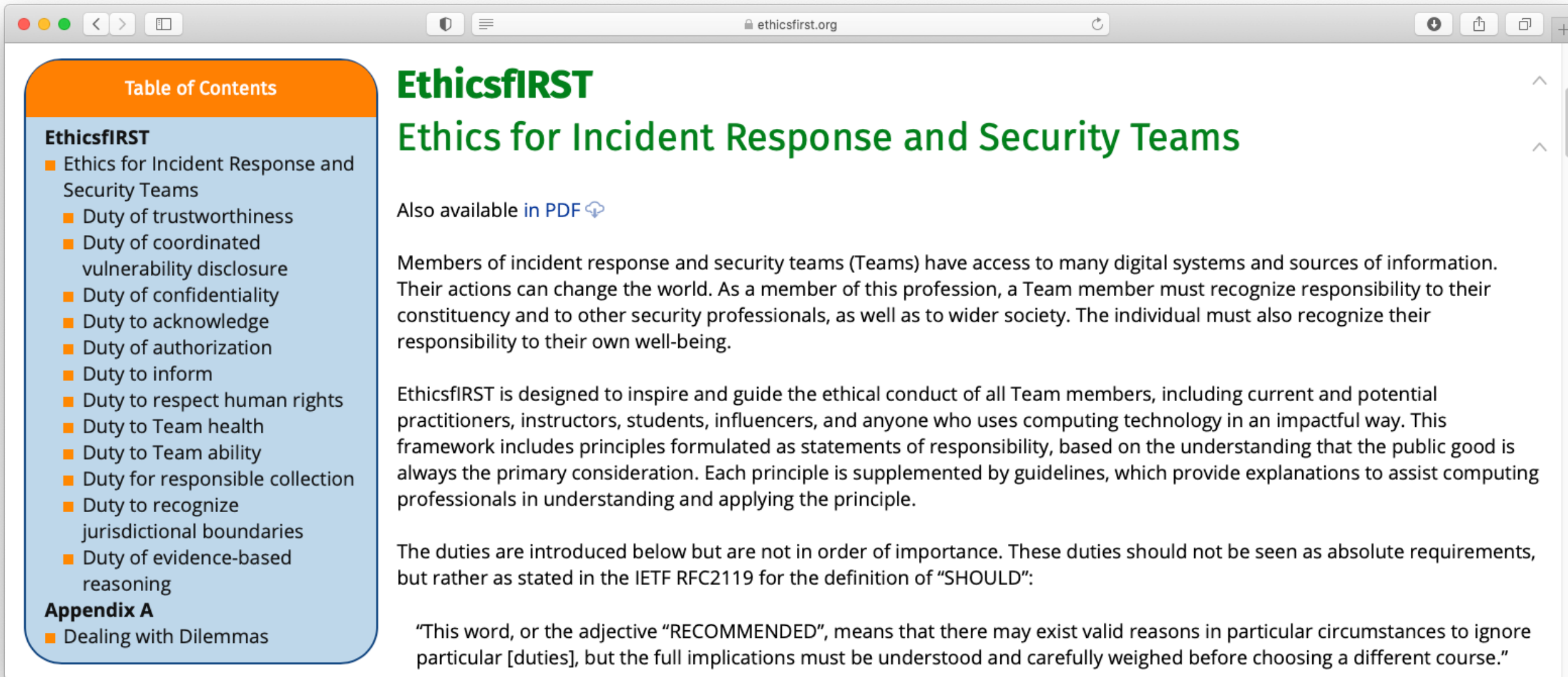
that Computer Security Incident Response Teams and other teams providing incident management related services may provide.”

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



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

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."

Gestão de Incidentes no Contexto da LGPD

cert.br nic.br egi.br

Incidente vs. Vazamento de Dados

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

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>

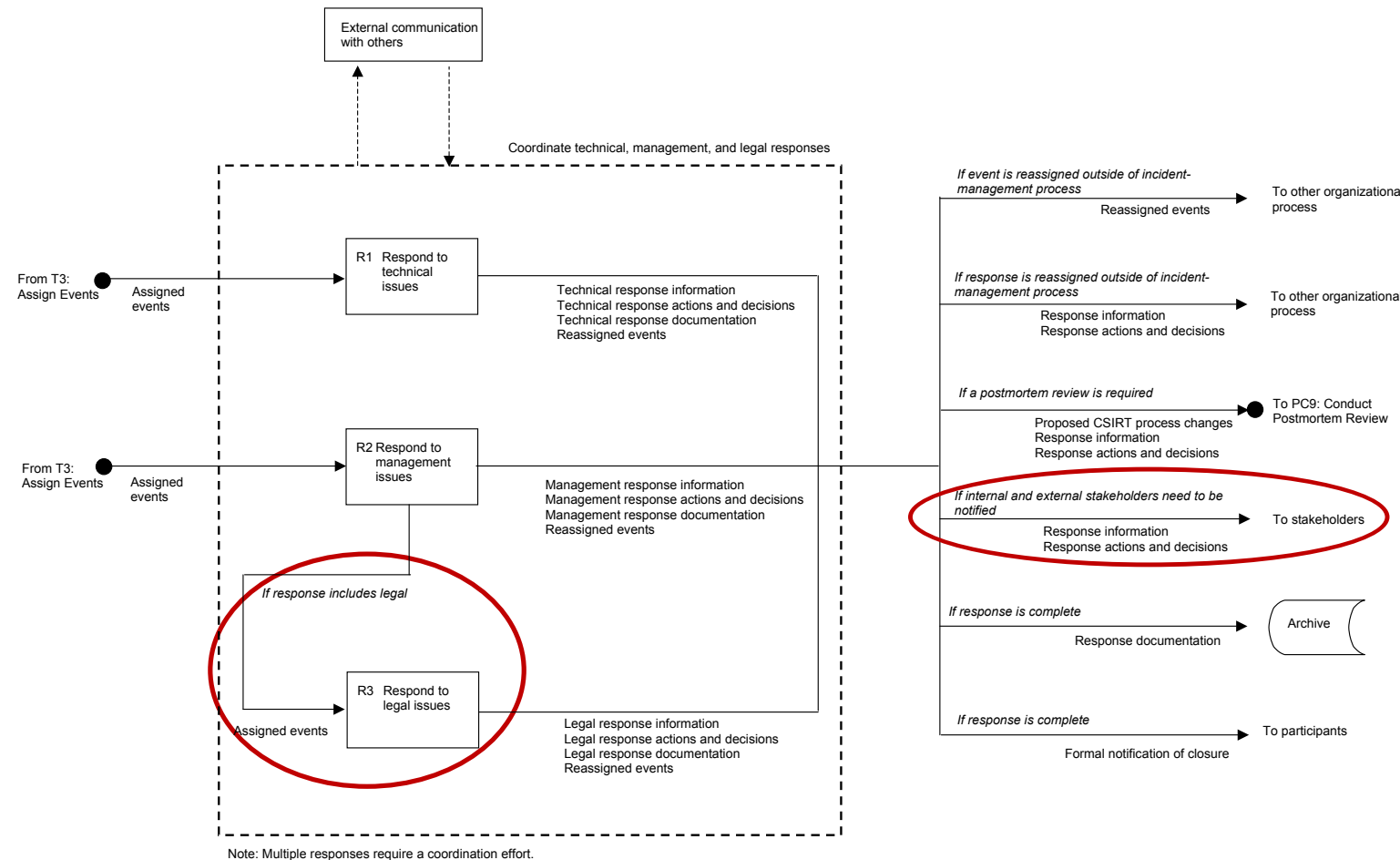
<https://cartilha.cert.br/fasciculos/#vazamento-de-dados>

https://csrc.nist.gov/glossary/term/data_loss

Incidentes Envolvendo Dados Pessoais ou Crimes: 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 técnica** ao incidente procura
 - identificar a causa raiz
 - identificar e mitigar os danos
 - recuperar o ambiente
- a **resposta legal** é uma decisão de cunho gerencial
 - uma equipe técnica não pode, por via de regra, decidir sozinha se é necessária uma resposta legal
 - os operadores da justiça e a ANPD são *stakeholders* externos a serem envolvidos em alguns casos
 - importante definir claramente em políticas o que fazer



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>

Nem todo incidente é crime ou envolve dados pessoais

Dia-a-dia do time 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 em casos como
 - quebra de contrato
 - crime
 - requerimento de órgãos reguladores
 - 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 ou possíveis crimes se diferencia apenas na fase final.

Por exemplo:

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

CSIRTs no Brasil

cert.br nic.br egi.br

CSIRTs com Responsabilidade Nacional

CERT.br / NIC.br / CGI.br

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/>

CTIR Gov / DSI / GSI / PR

Missão

Coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal (APF).

Público Alvo (*Constituency*)

Redes que fazem parte da Administração Pública Federal

Governança

Subordinado ao Departamento de Segurança da Informação (DSI), do Gabinete de Segurança Institucional (GSI), da Presidência da República (PR)

- responde diretamente à Assessoria Especial de Segurança da Informação do Ministro de Estado

<https://www.gov.br/ctir/pt-br/assuntos/abrangencia-operacional-constituency>
<https://www.gov.br/ctir/pt-br/aceso-a-informacao/institucional/organograma2>
<https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao>

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

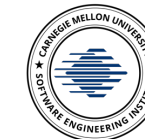
Criação:

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

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

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

Filiações e Parcerias



SEI
Partner
Network



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

Foco do CERT.br nestes 25 anos:

Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo 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 Resposta a 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

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

- EthicsFIRST
- SIM3 - *Security Incident Management Maturity Model*
- *TF-CSIRT Trusted Introducer*

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

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
- <https://cert.br/forum2022/>

Lista de CSIRTs Brasileiros

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

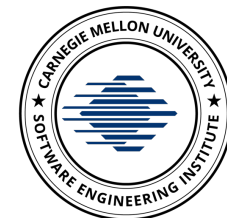
Fomento à adoção de MISP

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

Cursos de Gestão de Incidentes

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

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



SEI
Partner
Network

Iniciativas por Uma Internet Mais Resiliente

cert.br nic.br egi.br

Precisamos um Ecossistema mais Saudável: Faça a sua parte!



Programa nacional de incentivo à adoção de boas práticas:

Iniciativa:

- ISOC, NIC.br, CGI.br
Abranet, Abrint e Conexis

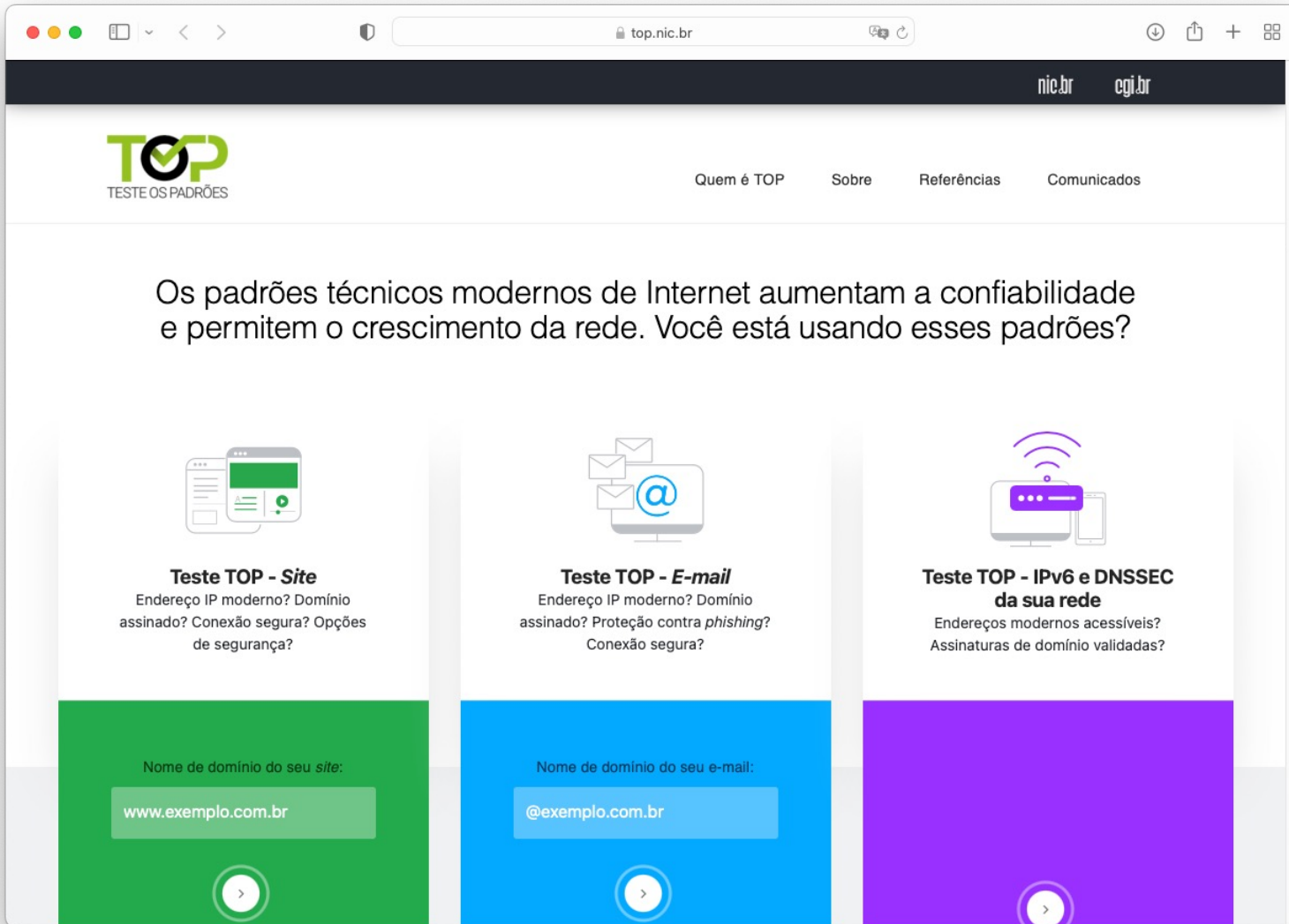
Apoio:

- InternetSul, RedeTelesul e TelComp



<https://bcp.nic.br/i+seg>

https://top.nic.br/ Testes para *site*, *e-mail* e conectividade



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

Apoiadores



Conscientização de Todos é Essencial: Portal InternetSegura.br – materiais gratuitos



<https://internetsegura.br/> – Todo o conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

Cartilha de Segurança para Internet: Fascículos e *Slides* para Palestras e Treinamento

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
- **Slides** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização

- Dica do dia no *site*, via *Twitter* e RSS
- Impressões em pequena escala enviadas a escolas e centros de inclusão digital
- Possível gerar versões personalizadas com logo da instituição

Exemplos de parceiros de impressão e distribuição:

Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

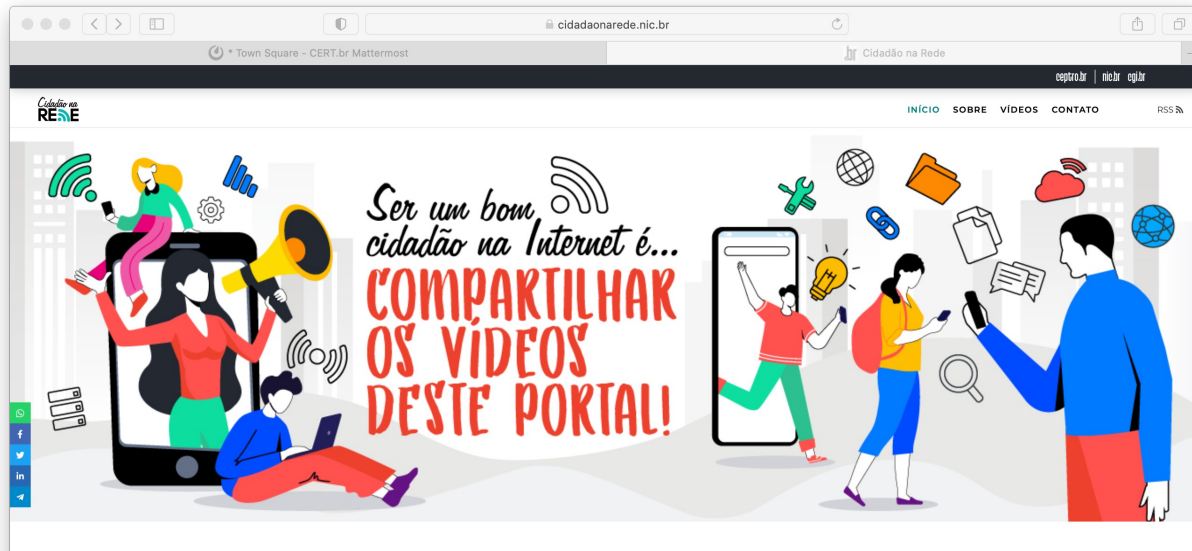


<https://cartilha.cert.br/>

Projeto Cidadão na Rede

“É direito e dever de cada pessoa ser um bom cidadão, e isso também vale para o mundo digital, usando de forma responsável as Tecnologias de Informação e Comunicação, em particular a Internet.”

- Conduzido pelo Ceptro.br
- Vídeos curtos sobre diversos temas:
 - Segurança
 - Infraestrutura da Internet e redes
 - Uso responsável e deveres na Internet



<https://cidadaonarede.nic.br/>

SEGURANÇA

Navegação segura
Tome cuidado com os sites que acessa. Será que eles são seguros? Entenda como identificar isso e navegar com segurança!
Postado em 22/10/2020

Gerenciador de senhas
Cada novo cadastro é mais uma senha para decorar. Quantas senhas uma pessoa comum consegue guardar na memória? Gerenciadores de senha estão aí para ajudar a administrar todas as senhas de maneira segura.
Postado em 22/10/2020

Verificação em duas etapas protege ainda + suas contas
Usar mais de um fator de segurança pode fazer a diferença na hora em que pessoas mal intencionadas tentarem invadir sua conta. Proteja suas contas!
Postado em 22/10/2020

Senhas Variadas
Na hora de criar uma nova senha sempre vem aquela vontade de usar uma das que você já utiliza, não é? Isso pode ser muito perigoso!
Postado em 22/10/2020

Senhas Seguras
Existem diversas práticas importantes para criar uma senha mais segura. Este vídeo mostra uma delas. Aprenda a proteger seus dados, criando boas senhas.
Postado em 22/10/2020

INFRAESTRUTURA DA INTERNET E REDES

A sua Internet pode ter cabo
Minha Internet parou... E agora?
Existem diversos motivos para sua Internet não estar funcionando. Mas, em alguns casos, basta reiniciar o roteador para a conexão voltar. Tente isso antes de ligar para o suporte.
Postado em 12/11/2020

Vídeos consomem muita "Internet"
Quando várias pessoas usam a Internet na mesma casa, a qualidade da rede para todos pode ficar comprometida. Isso acontece porque a quantidade de banda de Internet contratada pode não ser suficiente para atender a demanda.
Postado em 12/11/2020

Existem repetidores Wi-Fi
Os repetidores Wi-Fi possuem algumas limitações, uma delas é o alcance do sinal. Existem equipamentos simples para melhorar isso.
Postado em 12/11/2020

Sinal WiFi
Sabia que existem maneiras simples de melhorar o sinal do seu WiFi e com isso também melhorar a qualidade da sua navegação na Internet?
Postado em 12/11/2020

USO RESPONSÁVEL E DEVERES NA INTERNET

Nem tudo é brincadeira
Cyberbullying: e se fosse com você?
Não se deixe enganar, nem toda piada feita às custas de outra pessoa pode soar como uma simples brincadeira. O que pode parecer inocente ou muito engraçado para alguém, pode ter um impacto extremamente negativo no outro. Bullying ou Cyberbullying pode trazer consequências sérias.
Postado em 22/10/2020

A lei protege seus direitos também na Internet
Comprei on-line e me arrependi! O que fazer?
Fez uma compra on-line e se arrependeu, o que fazer? O Código de Defesa do Consumidor garante alguns direitos especiais para compras feitas fora do estabelecimento comercial, por exemplo, via Internet.
Postado em 22/10/2020

PODE SER UM ... BOATO
Boatos
A Internet está repleta de notícias, mas será que todas são verdadeiras? Cuidado ao compartilhar! E na dúvida, não compartilhe!
Postado em 22/10/2020

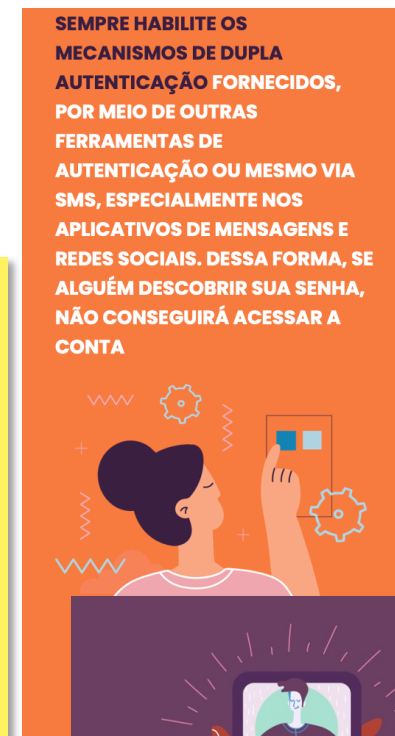
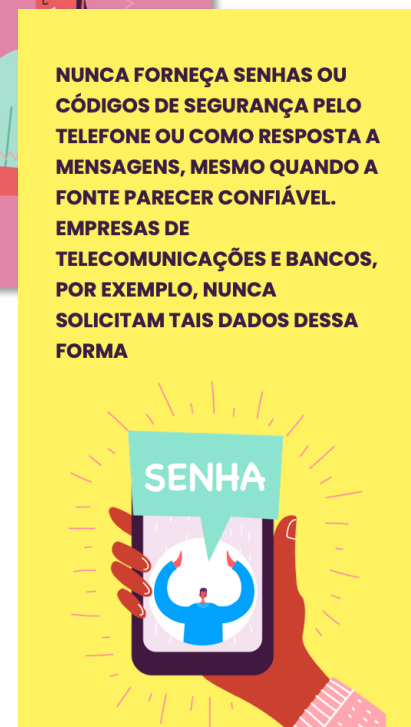
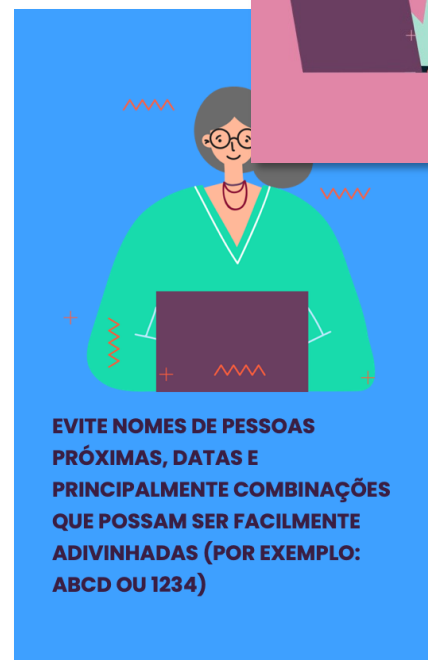
Campanha #FiqueEsperto

Iniciativa multissetorial em prol do uso seguro da Internet, com o objetivo de disseminar boas práticas

- Site com informações, divulgação via *e-mail*, via redes sociais e via mensagens (SMS) pelas operadoras de celular
- Apoiadores:
 - ABBC
 - Banco Central
 - Febraban
 - Abranet
 - CACB
 - ISOC Brasil
 - Abrint
 - camara-e.net
 - NIC.br
 - Anatel
 - Conexis
 - Telcomp
 - Assoc. Neo
 - CGI.br
 - WhatsApp



<https://fe.seg.br/>



Obrigada

✉ cristine@cert.br

✉ notificações para: cert@cert.br

📧 @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br