Cibersegurança: O Papel Essencial do Fator Humano

Miriam von Zuben

Analista de Segurança
CERT.br/NIC.br

Live Intra Rede – Ceptro.br/NIC.br
Evento *Online* – 14 de outubro de 2026

cert.br nic.br cgi.br

Desmistificando o Elo mais Fraco

1. The Persistent Myth of the "Human is Weakest Link"

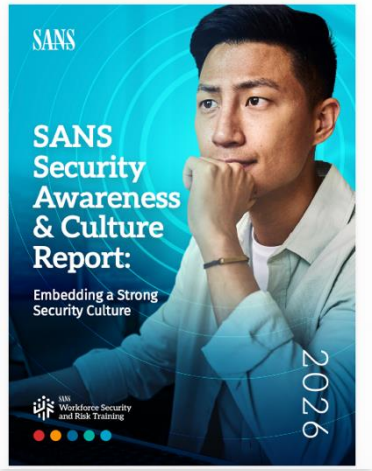
When an employee causes an incident, from falling victim to a vishing attack to accidentally sharing sensitive data in the cloud, far too often leaders perceive this as "the human is the weakest link." However, people are not the problem but, the environments we create are.

Security policies, tools, and expectations have become incredibly confusing, difficult and overwhelming for people. Yes, security is simple for most security professionals, but we live and breathe security daily.

People want to do the right thing, it's just that we have done a terrible job of communicating security in simple terms and making security as easy as possible. This is why people are not the weakest link; **they are the primary attack vector**. When people do cause an incident, instead of blaming them, we should be looking at the environment we have created and ask ourselves what we can do differently.

https://www.sans.org/blog/why-leadership-still-misunderstands-human-risk





https://www.sans.org/for-organizations/workforce/resources/security-awareness-report

Fortalecendo o Elo Humano

"Users are not the enemy.

They want to do their jobs,
and they want to do them securely

- if the security mechanisms do not make it impossible for them to work."

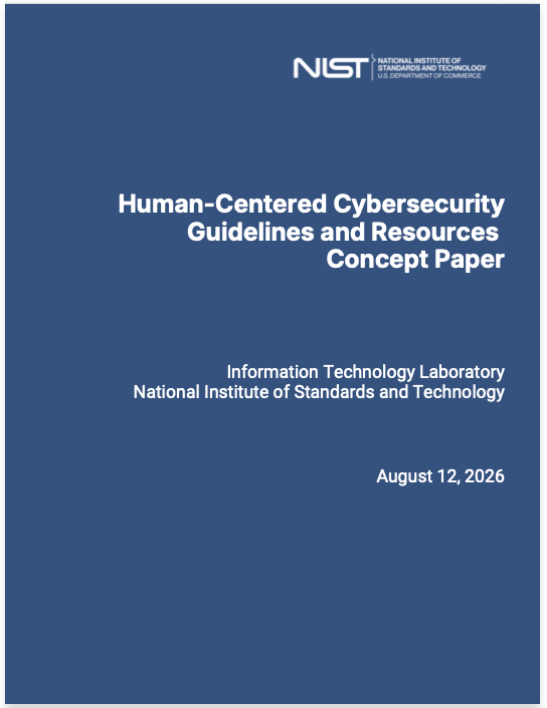
Anne Adams & M. Angela Sasse, 1999

https://doi.org/10.1145/322796.322806

Mudança de Paradigmas

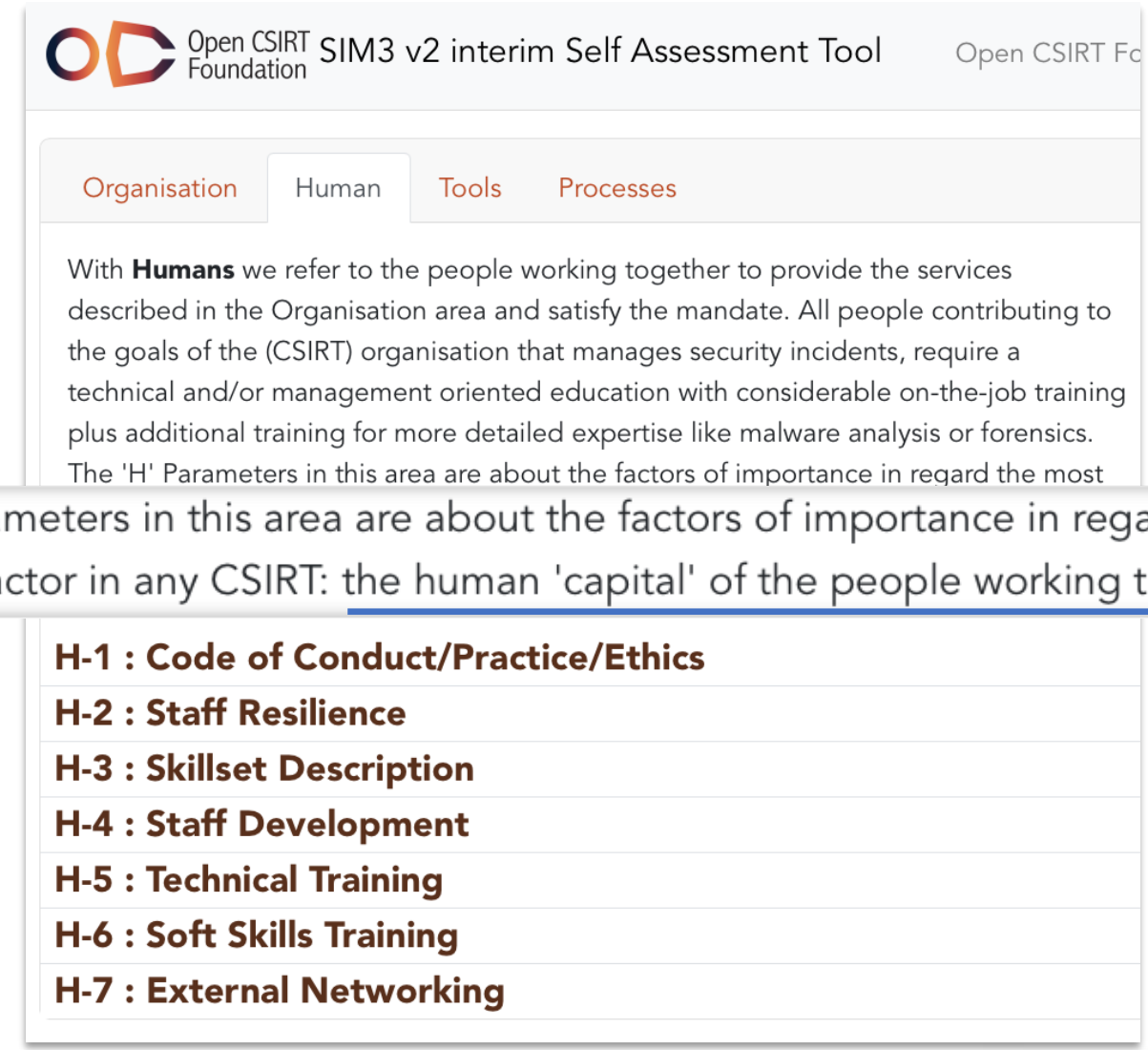
– Do tecnocentrismo:
  - pessoas como vetor de risco
  - abordagem punitiva
  - fadiga de alertas e sobrecarga de decisões
  - conscientização via longos treinamentos anuais

– À segurança centrada no humano (HCC):
  - pessoas como “primeira linha” e “sensor ativo” de defesa
  - maiores esforços em investigar as causas dos problemas e melhorar os sistemas
  - segurança *by design*, com configurações *default* mais seguras
  - orientações mais curtas, contextualizadas e oportunas
  - gamificação e atividades práticas para estimular engajamento e aprendizagem



https://csrc.nist.gov/projects/human-centered-cybersecurity/human-centered-cybersecurity-concept-paper

SIM3: O Fator Humano na Maturidade de um CSIRT



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

Mitigando *Insider Threats*

Definições SEI/CERT

*"A **malicious insider threat** is a **current or former employee, contractor, or business partner** who has or had authorized access to an organization's network, system, or data and **intentionally** exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems", 2012*

*"**Insider Threat** - the potential for an individual who has or had authorized access to an organization's critical assets to use their access, **either maliciously or unintentionally**, to act in a way that could negatively affect the organization", 2017*

*"**Insider Risk** - the impact and likelihood associated with the realization of an insider threat", 2026*

https://www.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/
https://www.sei.cmu.edu/documents/5777/5692_CSG_Book_20-optimized.pdf

Definições CISA

"An insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, negligent, or unintentional acts that negatively affect the confidentiality, integrity, and availability of the organization, its data, personnel, facilities, and/or associated resources.", 2026

"An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. An insider may be:"



A person the organization trusts and to whom the organization has provided sensitive information and access. This can include both full and part-time employees, contractors, and external third parties who still have some level of access



A person with regular or intermittent access to facilities and/or networks



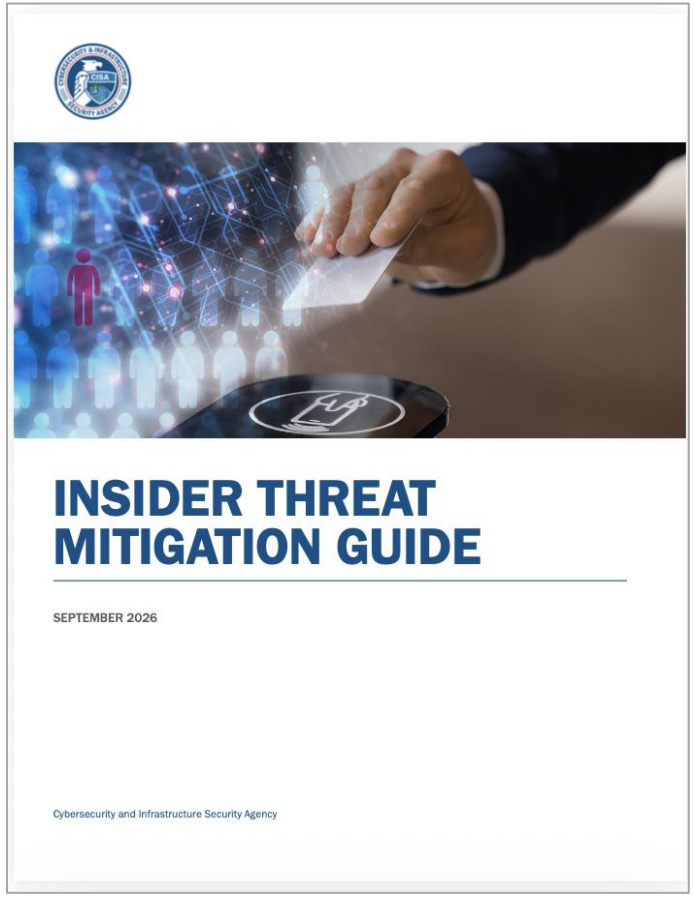
A person who develops the organization's products and services, including those who know the sensitive details of the products that provide value to the organization

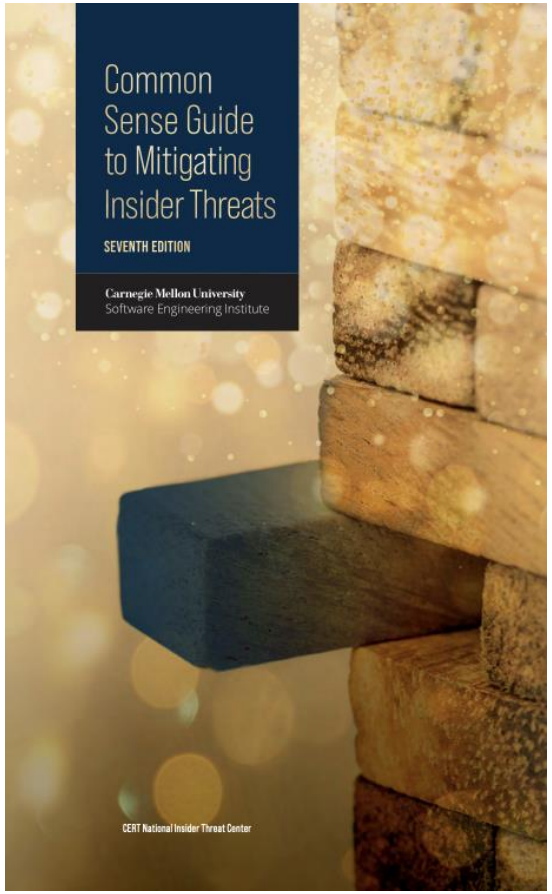


A person who is knowledgeable about the organization's fundamentals, including pricing, costs, and its strengths and weaknesses, and/or the organization's business strategy and goals

https://www.cisa.gov/sites/default/files/2026-09/cisa-insider-threat-mitigation-guide-2026.pdf

Insider Threat Mitigation Guides





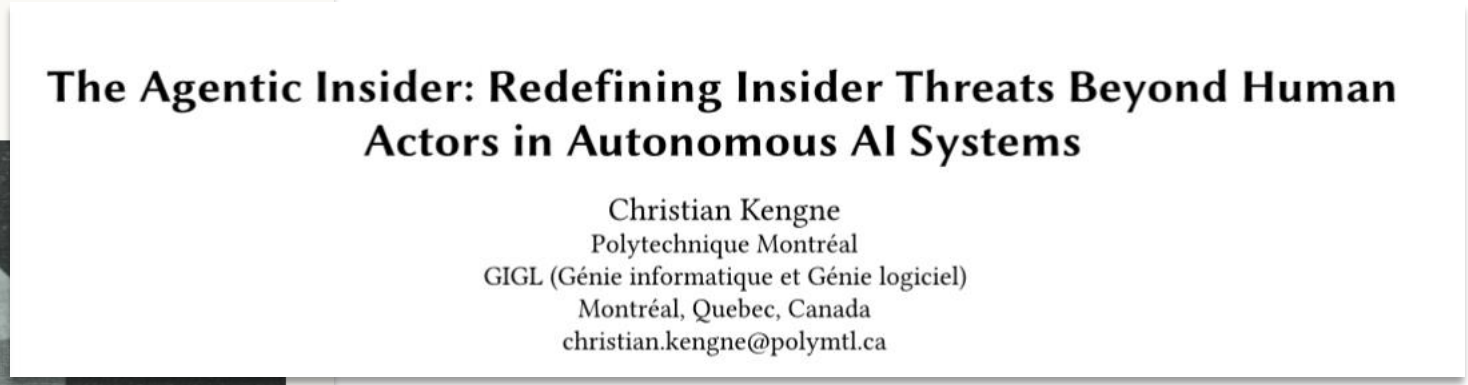
https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide
https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

Novos Desafios

Insider Threats e IA

Novos Desafios - *Insider Threats* e IA





https://www.anthropic.com/research/agentic-misalignment
https://dl.acm.org/doi/epdf/10.1145/3774905.3795476

“People are not the problem but, the enviroments we create are.”

Lance Spitzner

https://www.sans.org/blog/why-leadership-still-misunderstands-human-risk

Obrigada!

para materiais de conscientização: doc@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br