Prevenção de Incidentes além da Tecnologia

Cibelle Almeida

Cibelle Almeida

Administradora com atuação há mais de 20 anos diretamente com alta gestão de empresas de diversos mercados em reengenharia de processos, gerenciamento de Pessoas e treinamento, excelência na qualidade e melhoria contínua, dentre outros, com certificações DPO EXIN PDPF®, PDPP® e ISF®.
Atualmente pós graduanda em Proteção de Dados e Compliance Digital - Mackenzie.

Atualmente: Encarregada de Dados - DPO na Vaccinar Nutrição Animal.

Outras áreas de conhecimento em Proteção de Dados: Construção Civil - Engenharia Automação Industrial - Engenharia Ambiental - Jurídico - Representação Comercial - Saúde - Telecomunicação

TLP:CLEAR

CSIRT

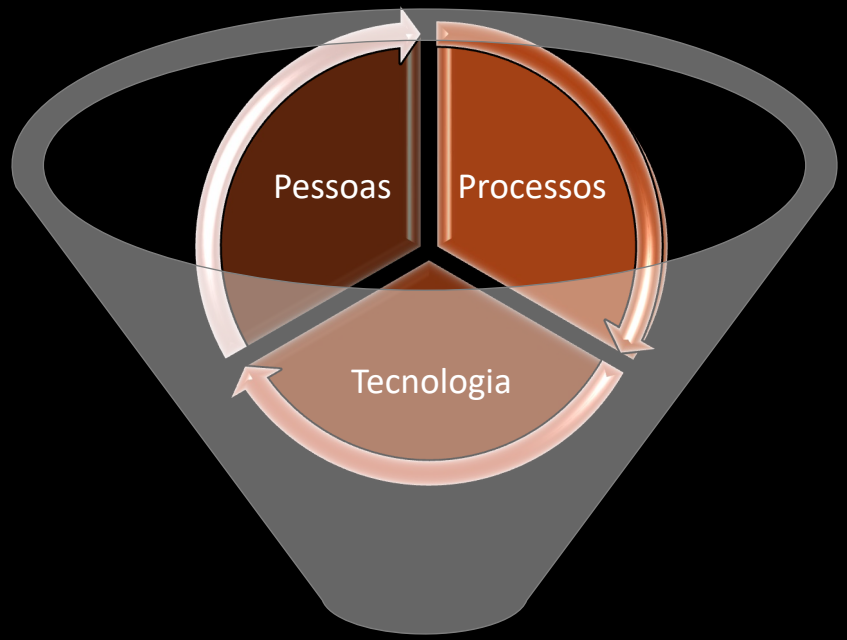
O CSIRT tem como OBJETIVO principal **identificar, analisar, gerenciar e responder a incidentes de segurança da informação** em uma organização.

plano de contingência | simulação | incidente

TLP:CLEAR

Tríade da prevenção

Análise



Implementação

Governança

TLP:CLEAR

além da tecnologia

- Padronização
- Procedimento
- Controle
- Monitoramento
- Auditoria
- Avaliação de Eficiência

TLP:CLEAR

Pontos de atenção

Backup
Antivírus
Infraestrutura
Classificação da Informação
Gestão de Acessos
APIs
Pentest
Exceções

TLP:CLEAR

Pontos de atenção comportamental

- Senha compartilhada
- Tela do computador aberta
- Documentos na impressora
- Gaveta sem chave
- Papel/documento solto em cima da mesa
- Papel no lixo
- Papel/documento inadequado usado como rascunho
- Equipe de limpeza interna ou externa sem treinamento
- Envio de dados pessoais/corporativos para e-mail pessoal ou indevido
- Postura no home office

TLP:CLEAR

7 princípios da metodologia Privacy By Design

ISO 31700

Ann Cavoukian

1. Proativo, e não reativo; preventivo, e não corretivo
2. Privacidade como padrão (Privacy by Default)
3. Privacidade incorporada ao design
4. Funcionalidade total (soma positiva, não soma-zero)
5. Segurança de ponta a ponta
6. Visibilidade e transparência
7. Respeito pela privacidade do usuário

Não é só tecnologia

- PSI
- Campanha Phishing
- Engenharia Social

TLP:CLEAR

Não é só tecnologia

COMPARTILHAMENTO INTERNO

COMPARTILHAMENTO EXTERNO

ARMAZENAMENTO

TLP:CLEAR

A segurança é um assunto amplo que abrange muito mais do que tecnologia. A cultura de segurança, treinamento, políticas e procedimentos claros, gestão de riscos, auditoria e conformidade, gestão de incidentes e comunicação eficaz são fundamentais para garantir que uma empresa esteja protegida contra ameaças de segurança.

TLP:CLEAR

Desafios

- Habilidades humanas.
- Tecnologia não adequada.
- Políticas e procedimentos inadequados.
- Conformidade regulatória: A não conformidade pode resultar em multas ou outras sanções legais, o que torna o cumprimento de regulamentos uma parte importante da segurança da informação.

ser HUMANO

- Falta de treinamento;
- Sobrecarga;
- Pressão, meta a cumprir;
- Piloto automático.

TLP:CLEAR

LGPD

- Agentes da Segurança: *hands-on*
- DPO itinerante
- Medidas Administrativas + Medidas Técnicas e Administrativas
- Campanhas de Segurança: vídeos Cidadão na Rede.
  https://cidadaonarede.nic.br/pt/

Próxima etapa

Apagar incêndio

Inteligência

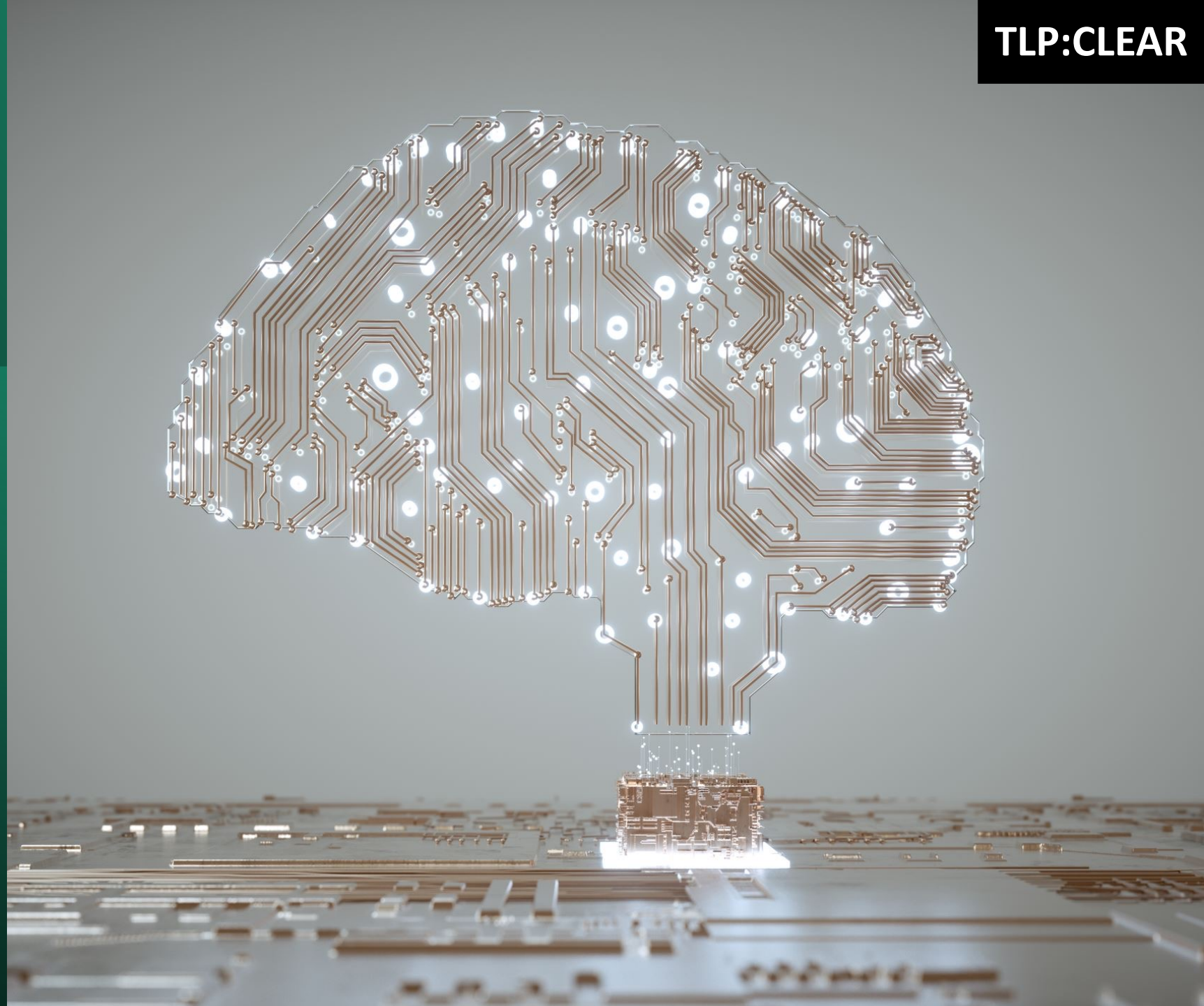
Contra inteligência

TLP:CLEAR

INTELIGÊNCIA

e

CONTRAINTELIGÊNCIA



TLP:CLEAR

INTELIGÊNCIA e CONTRAINTELIGÊNCIA são conceitos importantes em segurança além da tecnologia, pois muitas vezes as ameaças não vêm apenas de ataques cibernéticos, mas também de agentes internos ou externos que podem tentar obter informações ou prejudicar a organização de outras maneiras.

INTELIGÊNCIA é a capacidade de coletar, analisar e utilizar informações para tomar decisões informadas.

A CONTRAINTELIGÊNCIA compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de ações adversas que coloque em risco a Privacidade.

TLP:CLEAR

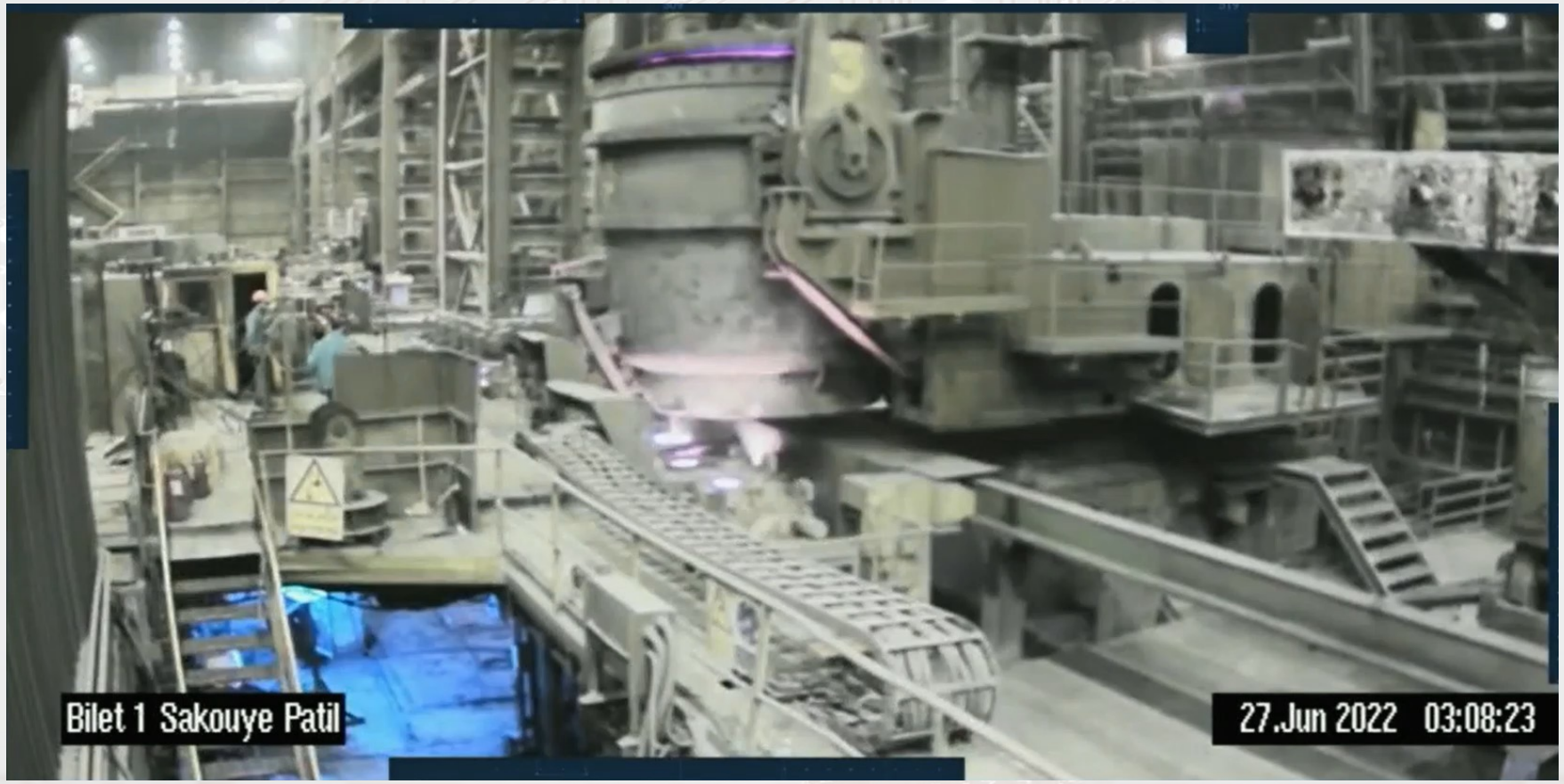
REGISTROS CORRETOS =
VIÉS DA SOBREVIVÊNCIA

PREVENÇÃO: segurança	SIMULAÇÃO
INCIDENTE	PLANO DE CONTIGÊNCIA
INTELIGÊNCIA	CONTRAINTELIGÊNCIA

Podem gerar **falsa segurança**:

- Não aplicar as práticas aprendidas, por exemplo, em cursos de Desenvolvimento Seguro;
- Assinar apenas um NDA sem implementar medidas administrativas e técnicas de segurança;
- Realizar Campanhas de *Phishing* sem ter um padrão de comunicação;
- Ter Políticas que existem apenas no papel;
- Utilizar ferramentas sem configuração correta;
- Ter KPIs sem uma finalidade definida.

ataque ciber-físico



Fonte: https://twitter.com/GonjeshkeDarand/status/1541288345183158272?s=20

ataque ciber-físico

- **TI**: em média **207 dias** para identificar e **70 dias** para conter, segundo a IBM.

- **OT**: **Às 13:23**, foi identificado um problema de resfriamento em um reator. **Às 13:33**, o reator estourou e seu conteúdo explodiu, matando 4 pessoas e ferindo 38 pessoas.

Fontes:
IBM. Cost of a data breach 2022. Online report: https://www.ibm.com/reports/ data-breach. Retrieved: May, 2023.
U.S. Chemical Safety and Hazard Investigation Board. T2 Laboratories Inc. Reactive Chemical Explosion: Final Investigation Report. https://www.csb.gov/t2- laboratories-inc-reactive-chemical-explosion. Retrieved: May, 2013. 2009.

TLP:CLEAR

consequências reais

MENU ASSINE

FOLHA DE S.PAULO

cotidiano > qualidade das praias educação coronavírus saúde ambiente mobilidade mortes

Suicídio de cirurgião investigado por morte de criança gera debate sobre saúde mental e papel da polícia e do jornalismo

Caso ocorreu um dia após a imprensa divulgar o indiciamento do profissional do Piauí por homicídio culposo

24.jul.2023 às 9h00

Cláudia Collucci

Fonte: https://www1.folha.uol.com.br/cotidiano/2023/07/suicidio-de-cirurgiao-investigado-por-morte-de-crianca-gera-debate-sobre-saude-mental-e-papel-da-policia-e-do-jornalismo.shtml

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.

St. Margaret's Health in Spring Valley, Ill. Google Maps

June 12, 2023, 12:25 PM -03

By Kevin Collier

Fonte: https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983

TLP:CLEAR

Utilizem a PREVENÇÃO e a CONTRA INTELIGÊNCIA para reduzir e controlar Incidentes de Segurança.
Vocês protegem PESSOAS!

Cibelle Almeida

Obrigada :)

https://www.linkedin.com/in/**cibellealmeida**