

# INEP



MINISTÉRIO DO  
**DESENVOLVIMENTO SOCIAL  
E AGRÁRIO**



# CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO – CTIR Gov



*Maj Democlydes Carvalho – Coordenador Geral*



# Todo líder de SI precisa saber responder essas questões

- *Você tem controle de todos os dispositivos conectados à rede?*
- *Onde estão seus dados e como são usados?*
- *Como seus usuários se comportam?*





# "WannaCry" ransomware attack losses could reach \$4 billion

MAERSK reports \$300M loss stemming from *NotPetya*

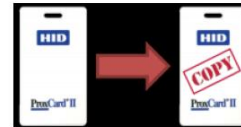


## Attack Tactics

1. Silently steal badge info



2. Create card clone



3. Enter and plant backdoor





No power To  
My Tablet  
Who can  
help me  
please ?

- ✓ 91% of attacks by cybercriminals start through mail
- ✓ Global cybercrime damage will exceed \$6 trillion annually by 2021
- ✓ The world will need to cyber defend X50 more data in 2021
- ✓ 110 billion human passwords and 200 billion machine passwords will require cyber protection by 2021
- ✓ Cybersecurity Ventures predicts global cybersecurity budget will exceed \$1 trillion from 2017 to 2021
- ✓ Microsoft Corp. will continue to invest over \$1 billion annually on cybersecurity R&D
- ✓ U.S. Government will invest over \$19 billion on cybersecurity for each President's Fiscal Year (FY) 2017



# 2016 Cybersecurity Skills Gap

## Too Many Threats

**\$1 BILLION:** PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014<sup>1</sup>

**97%** BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY<sup>2</sup>

**MORE THAN 1 IN 4** ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK<sup>3</sup>

**\$150 MILLION:** AVERAGE COST OF A DATA BREACH BY 2020<sup>4</sup>

**1 IN 2** BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES<sup>5</sup>

**74%** BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM<sup>6</sup>

## Too Few Professionals

**2 MILLION:** GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019<sup>7</sup>

**3X** RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14<sup>8</sup>

**84%** ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED<sup>9</sup>

**53%** OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES<sup>10</sup>

**77% OF WOMEN** SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.<sup>11</sup>

**89% OF U.S.** CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.<sup>12\*\*</sup>

**Cyberattacks are growing, but the talent pool of defenders is not keeping pace.**

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

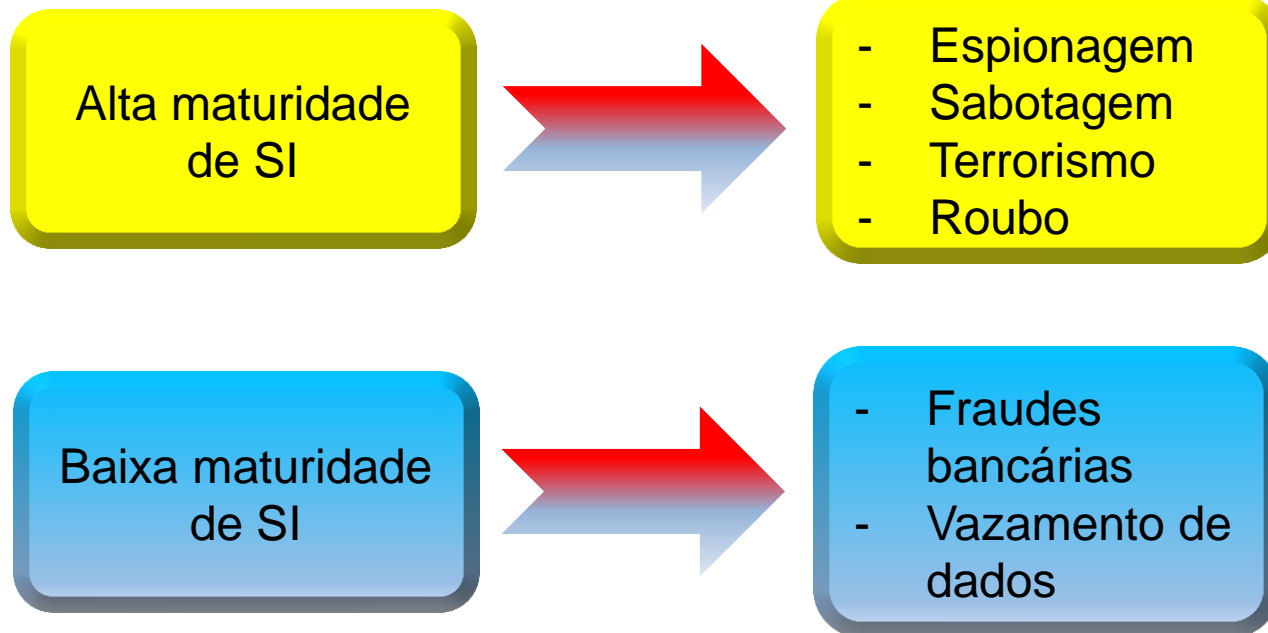
SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study, 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. ISACA 2015 IT Risk/Reward Barometer/Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer/Member Study. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer/Consumer Study, September 2015.



**There will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from 1 million in 2014.**

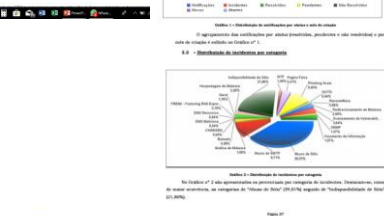
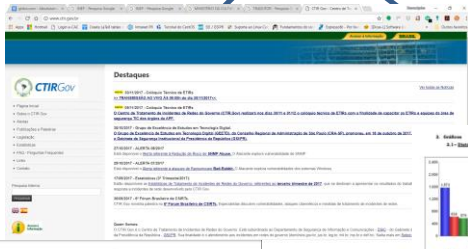
- *SENSIBILIZAÇÃO E MATURIDADE DE SI*
- *COLABORAÇÃO E COMPARTILHAMENTO*

## COMO AS AMEAÇAS SÃO VISTAS





# CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO – CTIR Gov



Regional Training Course on Computer Security for Industrial Control Systems at Nuclear Facilities

24 April 2017 to 28 April 2017 Rio de Janeiro, Brazil (D-TR-5549)

6º Fórum Brasileiro de CSIRT's



V SEMINÁRIO INTERNACIONAL de DEFESA CIBERNÉTICA

3º Fórum IBGP de Tecnologias da Informação



Visitas a 30 órgãos da APF  
Diagnóstico de Maturidade de Si  
**COORDENAÇÕES DSIC**



US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM



# Funcionamento / Formas de Contato



## Matriz de comunicação

- ✓ Sobreaviso
- ✓ INOC-DBA
- ✓ Telefones fixos



**Sobreaviso**  
Dias não úteis e dias  
úteis  
(após às 19:00 hs)

**Presencial**  
Dias Úteis  
(08:00 às 19:00 hs)

- <http://www.ctir.gov.br>
- [ctir@ctir.gov.br](mailto:ctir@ctir.gov.br) (notificação de incidentes)
- [democlydes.carvalho@presidencia.gov.br](mailto:democlydes.carvalho@presidencia.gov.br) (assuntos diversos)
- **INOC-DBA:** 10954\*810
- **Celular de Sobreaviso:** 61 99995-7859
- Para comunicação através de um canal seguro, por favor utilize a seguinte chave PGP:
  - PGP Key ID: 0xAFBEDFCF
  - Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF
  - PGP Public Key

ETIR-GOV mailing list

[ETIR-GOV@listas.planalto.gov.br](mailto:ETIR-GOV@listas.planalto.gov.br)

<https://www1.planalto.gov.br/mailman/listinfo/etir-gov>

**POLÍTICA  
NACIONAL DE  
SEGURANÇA DA  
INFORMAÇÃO  
(PNSI)**

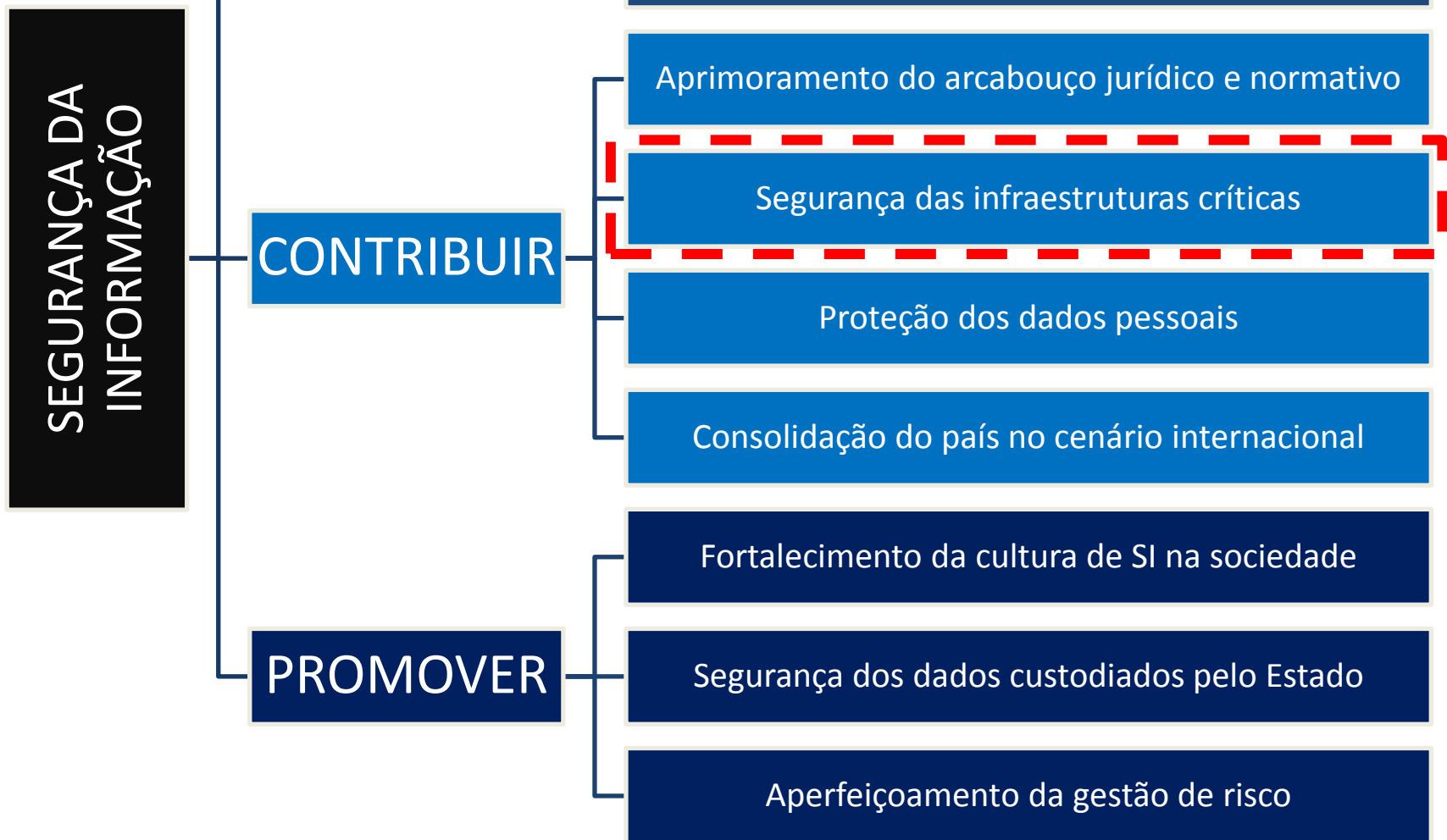




# PRINCÍPIOS



# OBJETIVOS



PÚBLICO

PRIVADO

SOCIEDADE

Direitos Fundamentais

Serviços Essenciais

Direitos Sociais

- Intimidade
- Vida privada
- Honra
- Imagem
- Acesso à informação
- Sigilo da correspondência
- Sigilo das comunicações
- Sigilo das votações



- Educação
- Saúde
- Alimentação
- Trabalho
- Previdência
- Transporte
- Segurança

(Lei 7.883/1989)

- Tratamento e abastecimento da água
- Produção e distribuição de energia elétrica, gás e combustíveis
- Assistência médica e hospitalar
- Distribuição e comercialização de medicamentos e alimentos
- Transporte coletivo
- Captação e tratamento de esgoto e lixo
- Telecomunicações
- Guarda, uso e comércio radioativos, equipamento e materiais nucleares
- Controle do tráfego aéreo
- Compensação bancária



# SEGURANÇA DA INFORMAÇÃO

ESPAÇO FÍSICO

ESPAÇO CIBERNÉTICO

# ESPAÇO CIBERNÉTICO MUNDIAL

## ESPAÇO CIBERNÉTICO BRASILEIRO



GS-PR  
(PNSI)

MD  
(MD31-P-02 - Política  
Cibernética de Defesa)

## DEFESA CIBERNÉTICA

ENERGIA

ÁGUA

TRANSPORTE

COMUNICAÇÕES

FINANCEIRO

### CIBERGUERRA

- Ataque Cibernético
- Proteção Cibernética
- Exploração Cibernética

MD  
(MD31-M-07 - Doutrina Militar  
de Defesa Cibernética)

## SEGURANÇA DA INFORMAÇÃO

### SEGURANÇA CIBERNÉTICA

- Dos processos
- Das pessoas
- Das tecnologias
- Dos ambientes

### DEFESA CIBERNÉTICA

## PRESSUPOSTO BÁSICO

A Segurança da Informação é a base da Defesa Cibernética e depende diretamente das ações individuais; não há Defesa Cibernética sem ações de SI.

*(MD31-P-02 - Política Cibernética de Defesa)*