

**MBA<sup>+</sup>**

**MBA em Gestão de Segurança da  
Informação**

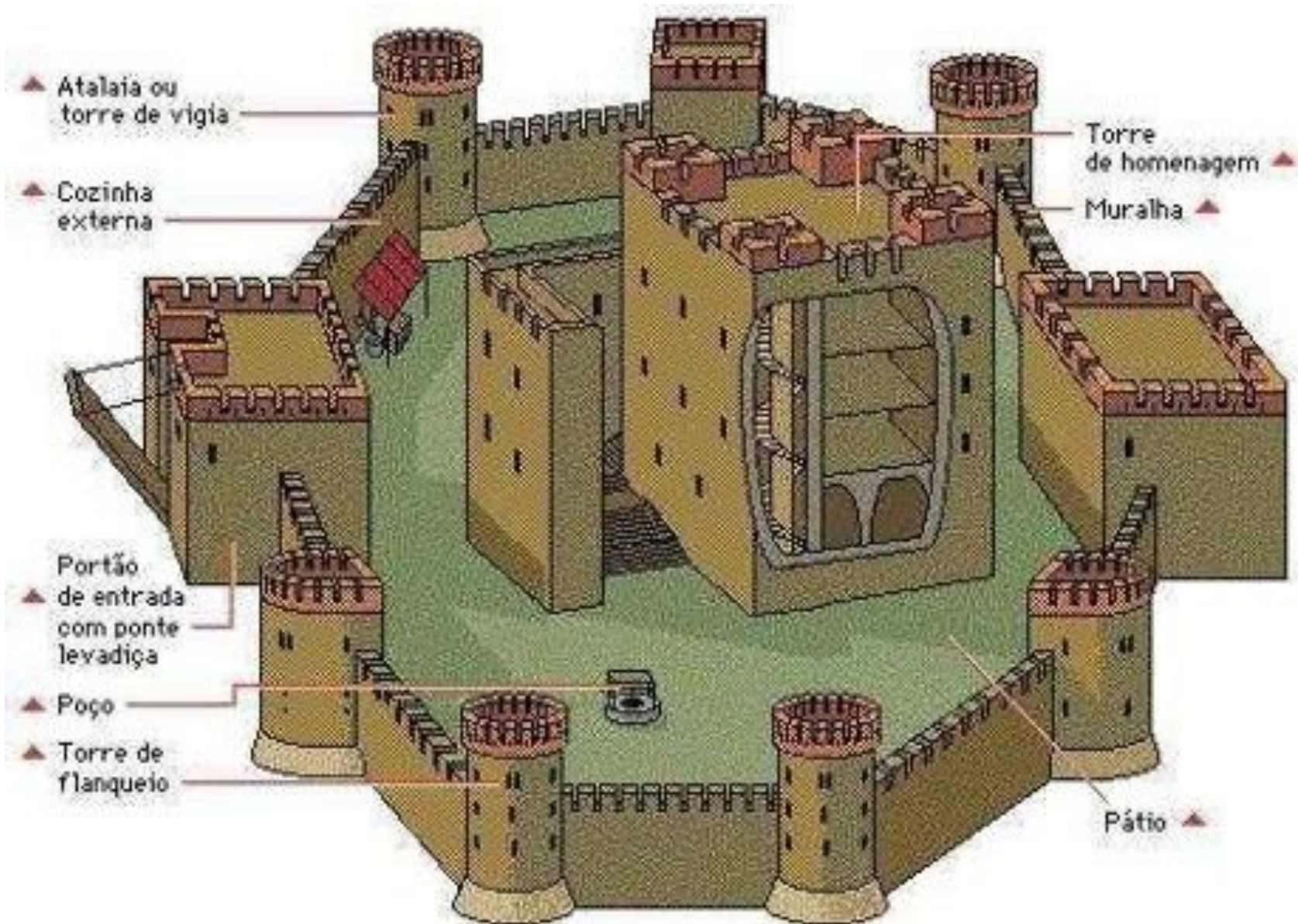
**MBA<sup>+</sup>**

# Physical and Environmental Security

**Prof<sup>a</sup> . Msc. Marcelo Barbosa Lima,**  
**CISSP, ISSAP, CISM, MBA**  
[mb\\_lima@uol.com.br](mailto:mb_lima@uol.com.br)

Agosto de 2023

# Sempre uma Prioridade





# **Segurança Física e Ambiental**



# Segurança Física

- Segurança Física é muito mais que Guardas, Armas e Portas.



# Segurança Ambiental



"Ainda que eu ande pelo vale da sombra da morte, não temerei mal nenhum..."

“Physical security protects people, data, equipment, systems, facilities and company assets. Methods that physical security protects these assets is through **site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection**”

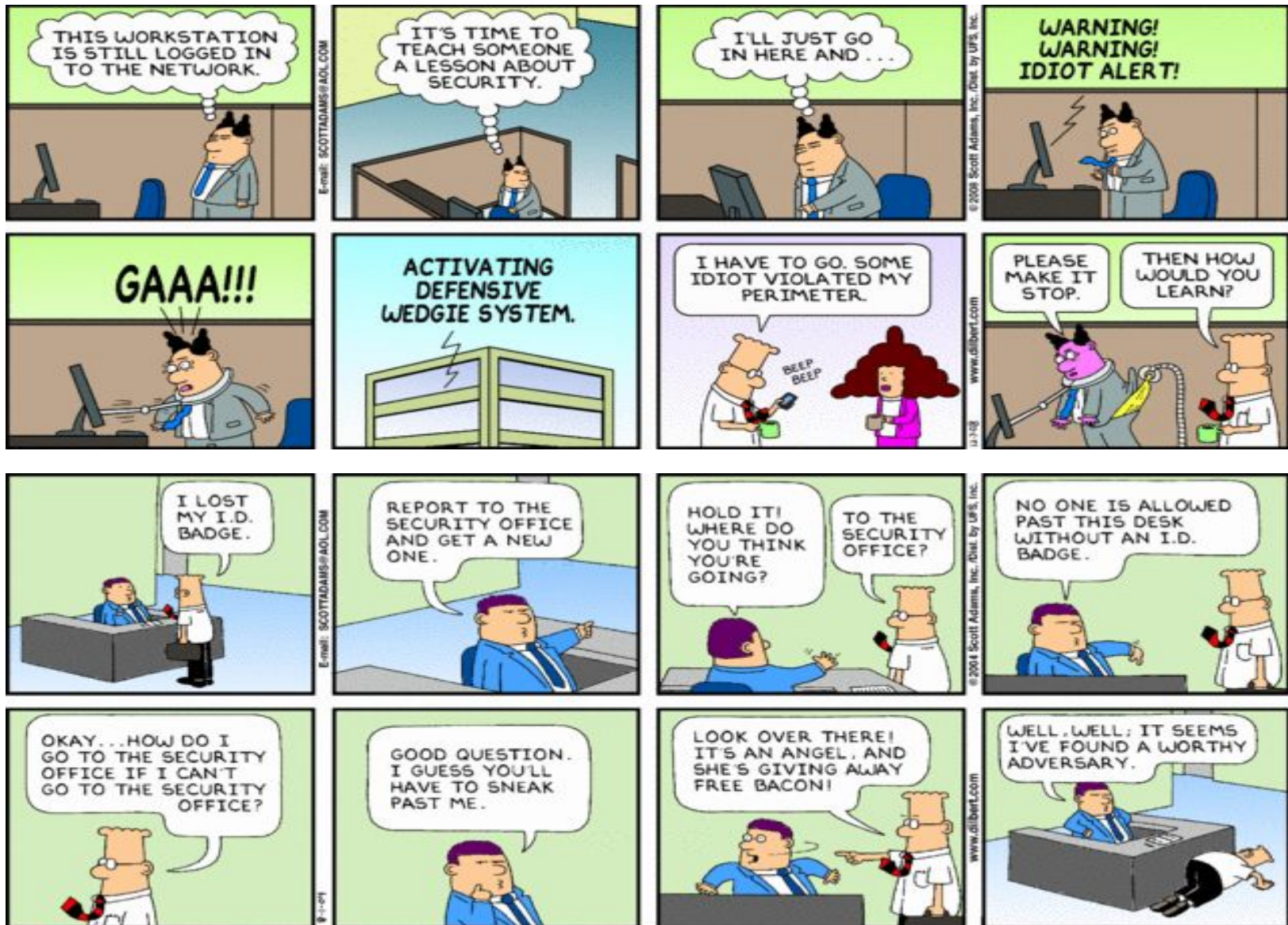
(Harris, 2013)

“Physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, **it is often overlooked because most organizations focus on “technology-oriented security countermeasures to prevent hacking attacks”**

**(Harris, 2013)**



# Controles Administrativos



# Algumas Normas

- ISO 27001
- SSAE 16 (antiga SAS 70)
- PCI DSS
- ANSI/TIA-942-A
- ...



# **Algumas Ferramentas no Arsenal do Red Team e dos Black Hats**



# Implantes de Hardware

FIAP





## Favourites

Favorite list is empty.  
[Clear favorites](#)

## Latest News on CBR

Imperva Hacked: Customer API Keys, SSL Certificates Stolen  
[6 hours ago](#)

Gov't Plans to Slash 5G Mast Red Tape: Launches £30m Rural 5G Fund  
[10 hours ago](#)

VMware: vSphere's Going Kubernetes-Native  
[11 hours ago](#)



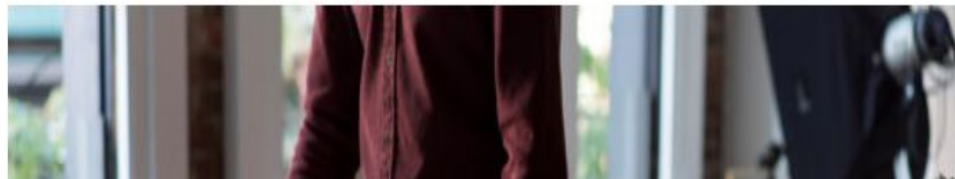
THREATS

[Back to Home](#)

# IBM Says the Parcel is your Next Threat Vector: Posts \$100 Hacking Device to Crack Sensitive Networks

CONOR REYNOLDS  
7TH AUGUST 2019

+ INCREASE / DECREASE TEXT SIZE -



## MOST READ



Imperva Hacked: Customer SSL Certificates Stolen  
ED TARGETT 27TH AUGUST 2019



VMware: vSphere's Going



# Kit de Ferramentas - Com Engenharia Social

FIAP



# Weaponization de devices USB


FIAP






# Documentário Recomendado

FIAP




Prime Video ▾

Q

EN  Hello, Marcelo 

Account & Lists ▾

Returns & Orders

0  Cart


Today's Deals Marcelo's Amazon.com Help Browsing History ▾ Registry Buy Again Gift Cards Sell 

Shop Today's Deals

prime video Home Channels Rent or buy Categories ▾ My Stuff 

Settings Getting Started Help

## Hacking the Grid

★★★★☆ (40) 16min 2016 ALL 

A power company in the Midwest hired a group of white hat hackers known as RedTeam Security to test its defenses. We followed them around for 3 days, as they attempted to break into buildings and hack into its network, with the goal of gaining full access. It was much easier than you think.

This title isn't available in your location

Remove from Watchlist

Genres

Special Interest


Director


Chris Snyder, Paul Szoldra


Starring

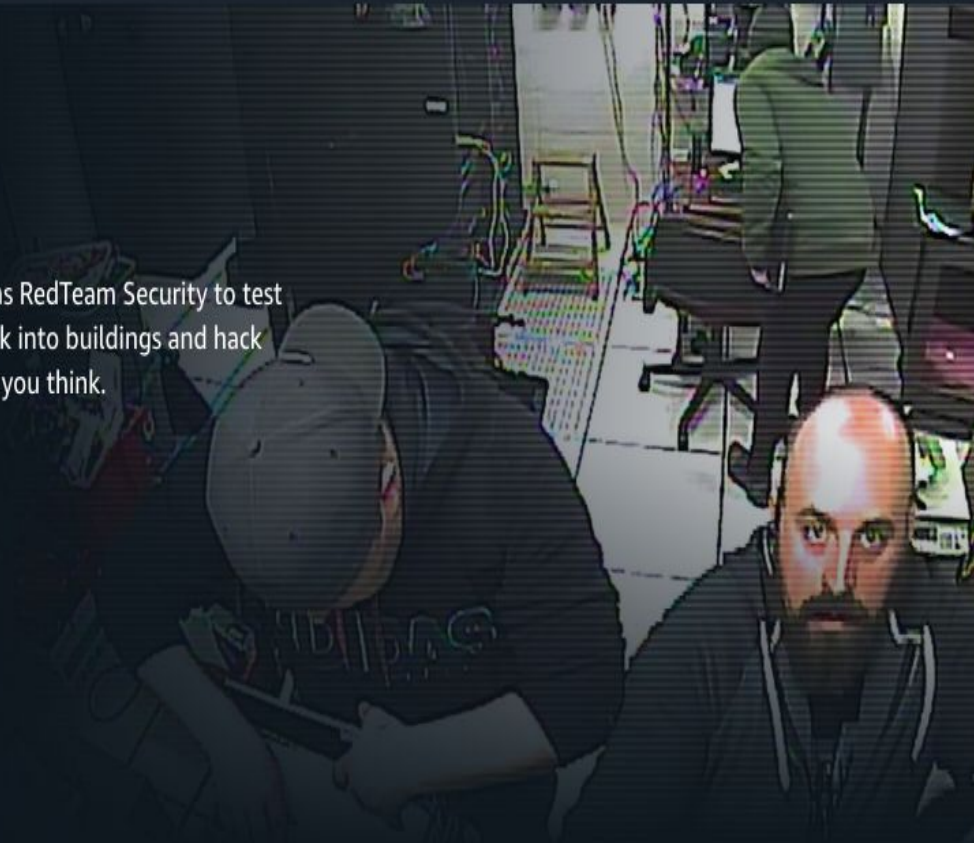
Jeremiah Talamantes, Ryan Manship

By ordering or viewing, you agree to our [Terms](#). Sold by Amazon Digital Services LLC.

 Share

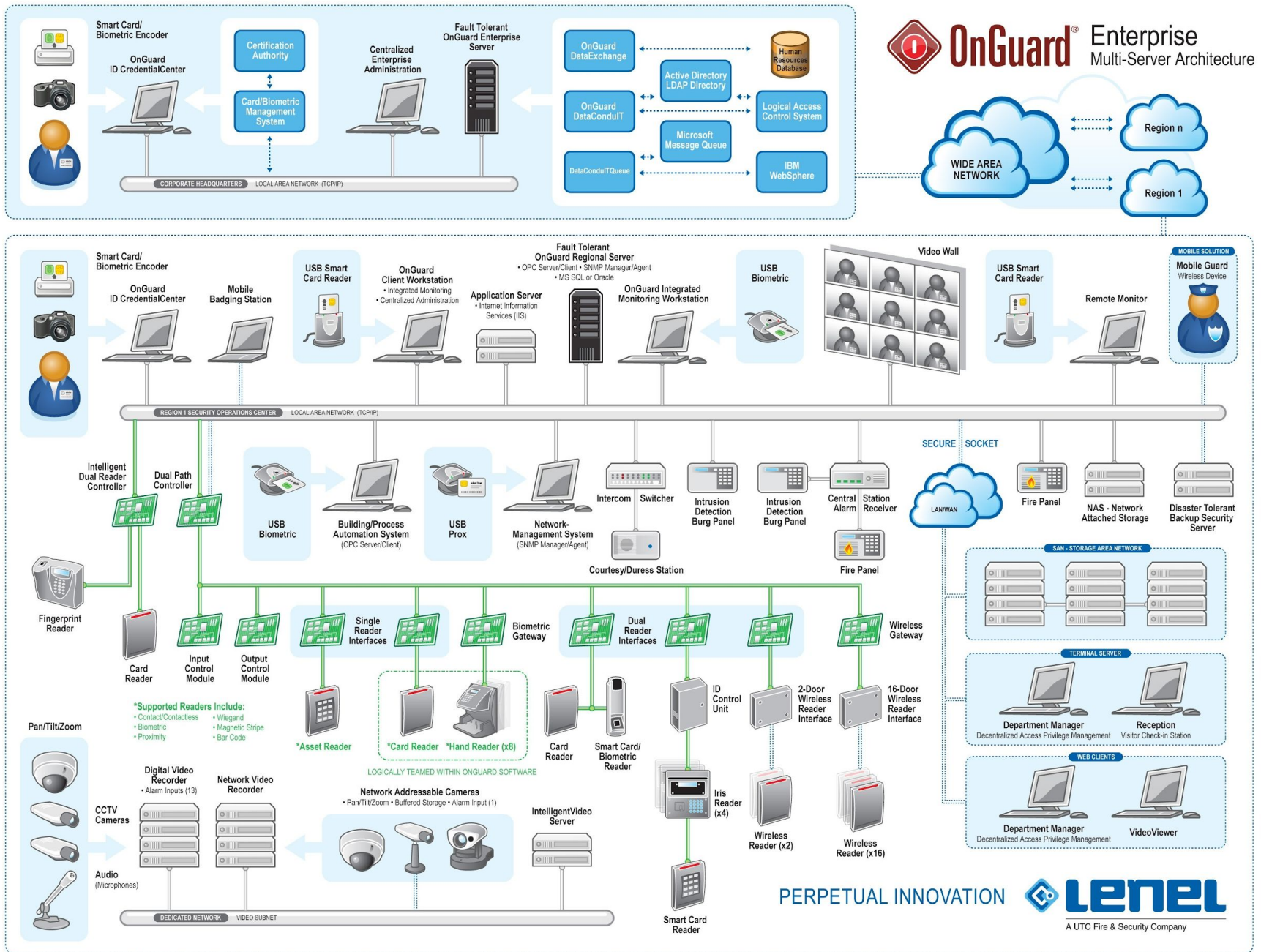
 Feedback

 Get Help



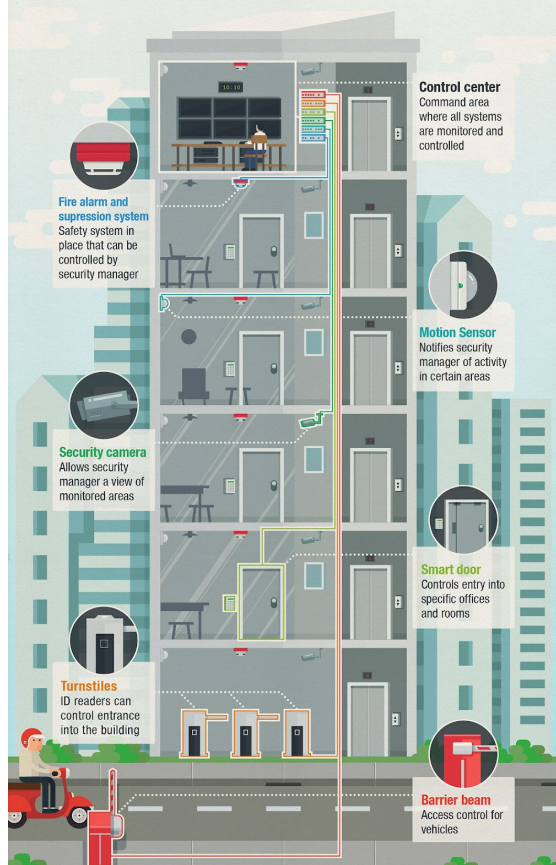


# **Controles de Segurança Física usados como backdoors**





## PROTECTING PHYSICAL SECURITY SYSTEMS AGAINST NETWORK ATTACKS



### Manage and Secure your Devices

#### Network segmentation

- Configure VLANs and install firewalls
- Monitor networks for anomalous activity

#### Firmware updates

- Find out who is responsible for managing your firmware
- Make sure you have the latest updates

#### Proactive assessment

- Find vulnerabilities and address them before they are exploited
- Perform penetration testing against your environment

#### Device auditing

- Before deploying devices check the level of encryption and if there are proper authentication features

**Think before you link!** Security devices help ensure the safety of everyone in the building, but are you sure that these devices need to be networked? Weigh the pros and cons of having IoT security devices.

## Cuidados Necessários



- Segregação da Rede
- Emprego de sistemas de detecção de anomalias/intrusos
- Atualização contínua dos firmwares/softwarees dos dispositivos
- Mudança dos parâmetros default dos diferentes dispositivos
- Restrição de acesso de IPs remotos
- Uso de múltiplos fatores de autenticação
- Utilização de VPN para acesso remoto
- Alertas enviados para o SOC
- Proteção do Sistema de Gerenciamento dos dispositivos



# **Ataques Físicos e Dispositivos**

# Ataques Físicos a Devices

FIAP

TECMUNDO

Curtir 6,2

NOTÍCIAS ▾

COMPARAR CELULARES

VOXEL

TECMUNDO TV

CUPONS DE DESCONTO

THE BRIEF

## GrayKey: essa caixinha promete ser capaz de invadir até mesmo o iPhone X

POR FELIPE AUTRAN - EM SEGURANÇA - 16 MAR 2018 — 10H25



COMPARTILHAR



G+

in

16

275 compartilhamentos





BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FO

BREAKING AND ENTERING —

## Cellebrite can unlock any iPhone (for some values of “any”)

Forensics contractor’s “Advanced Unlocking Service” still has to brute-force passcodes.

SEAN GALLAGHER - 2/28/2018, 10:50 PM



# Evil Maid Attack



Backdoor pode ser obtida em <https://github.com/cr4sh/smmbackdoor>



# Evil Made Attack

FIAP

## SF600 SPI Flash IC Programmer

Model Name : SF600

Other than ICP Programming, it also supports socket adaptor programming.



USD\$285

-

1

+

Add to Cart

Description

Media

ECN

### Feature

The SF600 is a high speed "in System Programming" programmer to update the SPI Flash soldered on board (In-Circuit Programming) or in the socket adaptor (Offline programming). The programmer is easily controlled by the computer DediProg Software through the USB bus offering a friendly interface and powerful features to users.

SF600 combines the advantages of SF100 with additional improvements: High-speed USB and higher SPI performances.



Highlights

## The Hacker News

Subscribe to Newsletter

Home

Data Breaches

Cyber Attacks

Vulnerabilities

Malware

Offers

Contact



**mimecast**

**Deep insights, better  
visibility, reduced risk**

Resources on governance, compliance & data protection.

GET RESOURCES

## New 'MosaicRegressor' UEFI Bootkit Malware Found Active in the Wild

October 06, 2020 Rave Lakshmanan



# Bypass de Sistemas de Autenticação

FIAP

 **TECMUNDO**

 Curtir 6,2 mi 

NOTÍCIAS ▾

COMPARAR CELULARES

VOXEL

TECMUNDO TV

CUPONS DE DESCONTO

THE BRIEF



**Kaspersky®  
Internet Security**

Proteja seu computador e  
seus dados pessoais das  
ameaças digitais.

**COMPRE AGORA**

**KASPERSKY**

## A incrível ferramenta para burlar o Apple Face ID: um boné

POR [FELIPE PAYÃO](#) | [@felipepayao](#) - EM [SEGURANÇA](#) - ⓘ 22 MAR 2018 — 18H45

# Juice Jacking

FIAP



BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS

jui

1/1 | ^ v x



  
CROWDSTRIKE

NAMED HIGHEST IN **EXECUTION & FURTHEST IN VISION**  
VISIONARIES QUADRANT, GARTNER MAGIC QUADRANT FOR EPP

AdChoices

GET REPORT

## Please stop charging your phone in public ports

by [Selena Larson](#) @selenalarson

🕒 February 16, 2017: 10:37 AM ET

 Recommend 18K





# Atacando “Air-Gapped” Devices

FIAP

## MOTHERBOARD

LATEST



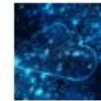
How Self-Driving Car Policy Will Determine Life, Death and Everything In-Between



Guccifer 2.0 Was Always Sloppy



California Lawmakers Want Twitter Bots Branded With Disclaimers



Congress Enacts Garbage Surveillance Legislation By Attaching it to Must-Pass Budget Bill

## New Hack Can Steal Data From Devices in Faraday Cages

Last year Wikileaks released documents detailing how attackers can compromise offline computers. This new study goes one step further, exposing the fallibility of Faraday cages



# Atacando “Air-Gapped” Devices

FIAP

Home Hacking Tech Deals Cyber Attacks Malware Spying



G+  
+1,699,900

Twitter  
455,000

f  
2,095,600

**Jeep Compass  
Trailhawk**

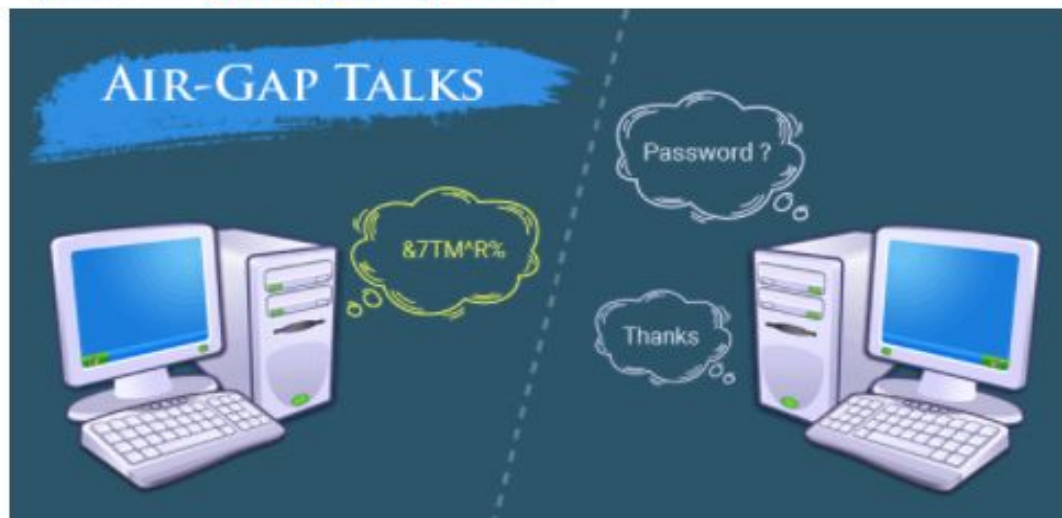
Tração 4x4 com  
seletor para até  
5 tipos de terrenos.

MONTE O SEU  
**Jeep**

## MOSQUITO Attack Allows Air-Gapped Computers to Covertly Exchange Data

Monday, March 12, 2018 Mohit Kumar

Share 4.01k Share Tweet Share



# Jumping the Air-Gap with a small Hard Drive LED

FIAP

paper: <https://arxiv.org/abs/1702.06715>



A drone is navigated to a line-of-sight  
with the infected computer

# IMSI Catchers

FIAP

Home Hacking Tech Deals Cyber Attacks Malware Spying



G+  
+1,699,900

Twitter  
455,000

f  
2,095,600



**Equinix Hybrid Cloud**

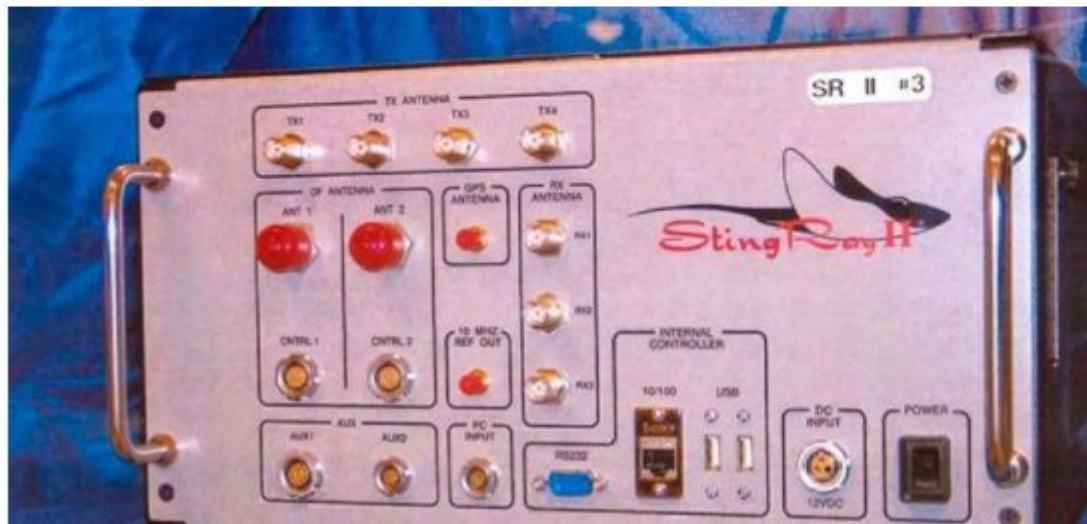
Conexão privada com os principais Cloud Providers e gestão multicloud em um único portal



## Local Police Listening Your Cell-Phone Without a Warrant

Thursday, April 09, 2015 Mohit Kumar

Share 1 in Share Tweet Share



**One Giant Leap for Security**

Discover the Next Frontier of Threat Detection and Incident Response

 ALIEN VAULT

**LEARN MORE**

**0%** NOVA FIAT COM TAXA

COM CÂMBIO AUTOMÁTICO E IPVA GRÁTIS


**ARGO 1.8**





# IMSI Catchers

FIAP

ars TECHNICA


[BIZ & IT](#) [TECH](#) [SCIENCE](#) [POLICY](#) [CARS](#) [GAMING & CULTURE](#) [FORUMS](#) [SUBSCRIPTIONS](#) [SIGN IN](#)


BIZ & IT —

## Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations

\$1,400 device can track users for days with little indication anything is amiss.

DAN GOODIN - 10/28/2015, 10:59 AM



CROWDSTRIKE

76%

OF ENTERPRISES  
ARE REPLACING  
AV IN 2018

GET BETTER ENDPOINT PROTECTION

15-DAY FREE TRIAL





**Elo mais Fraco**

# Fotos em Áreas Restritas

FIAP



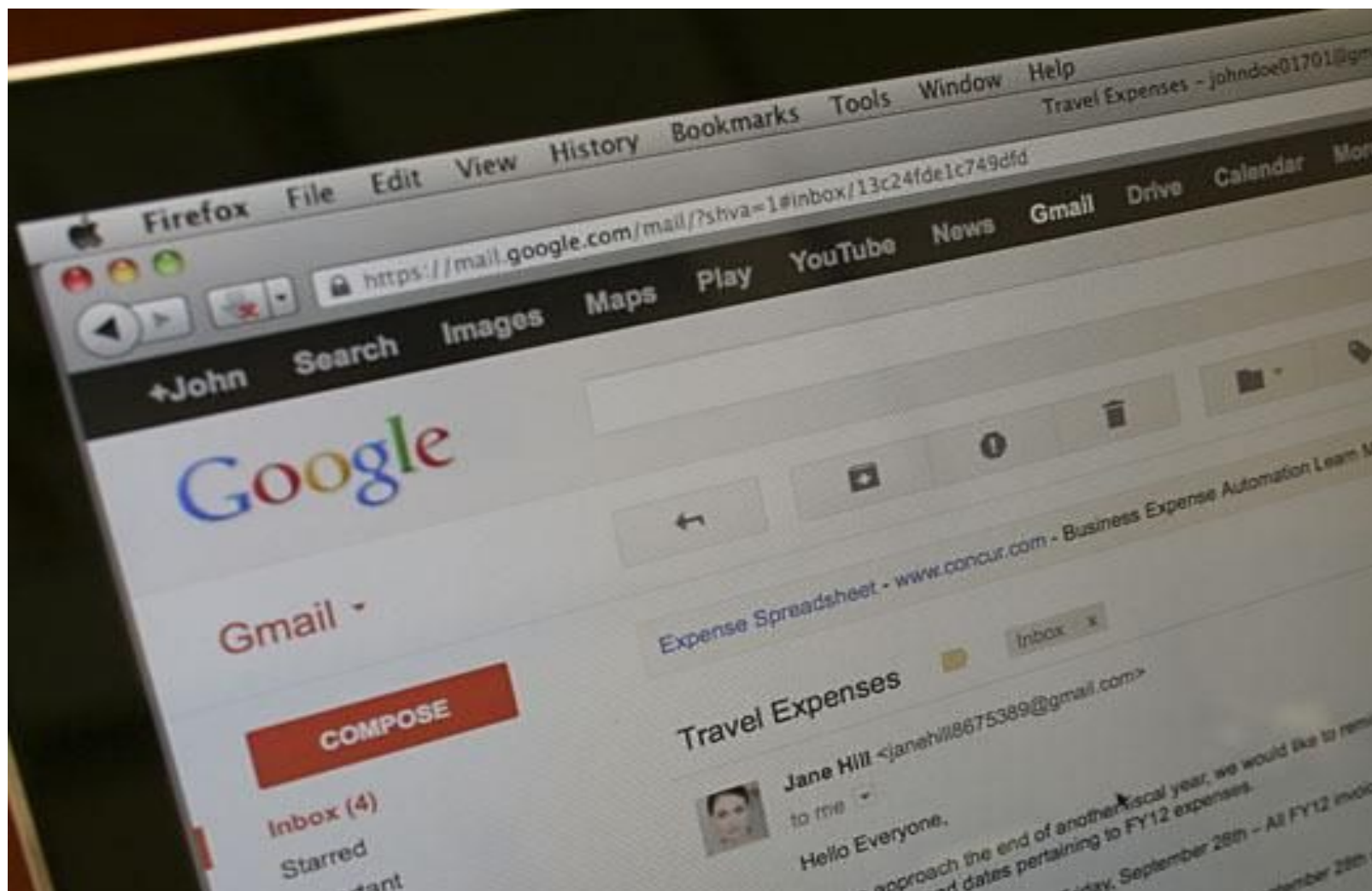
# Mesa Limpa

FIAP



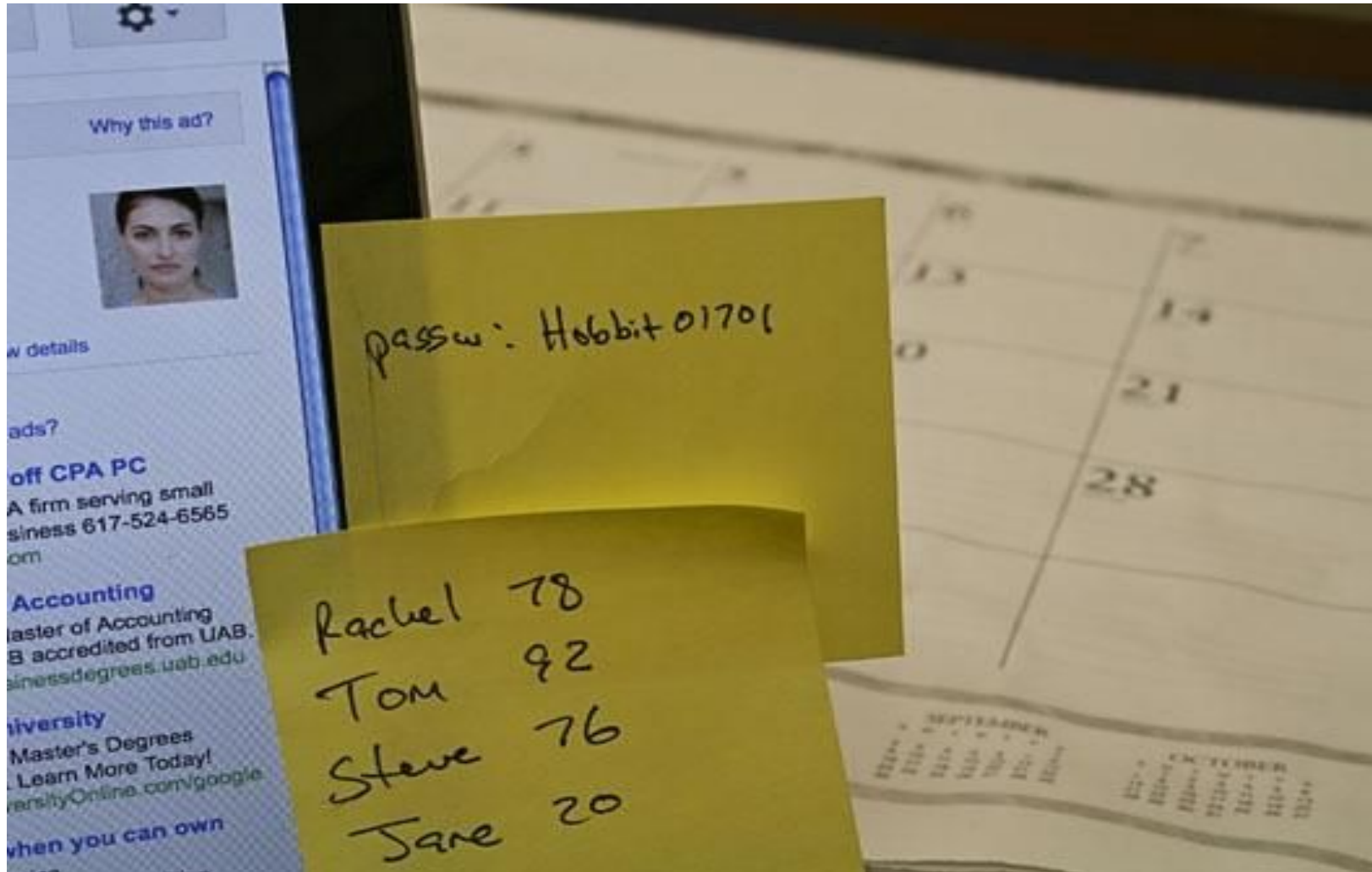
# Bloqueio de Tela

FIAP



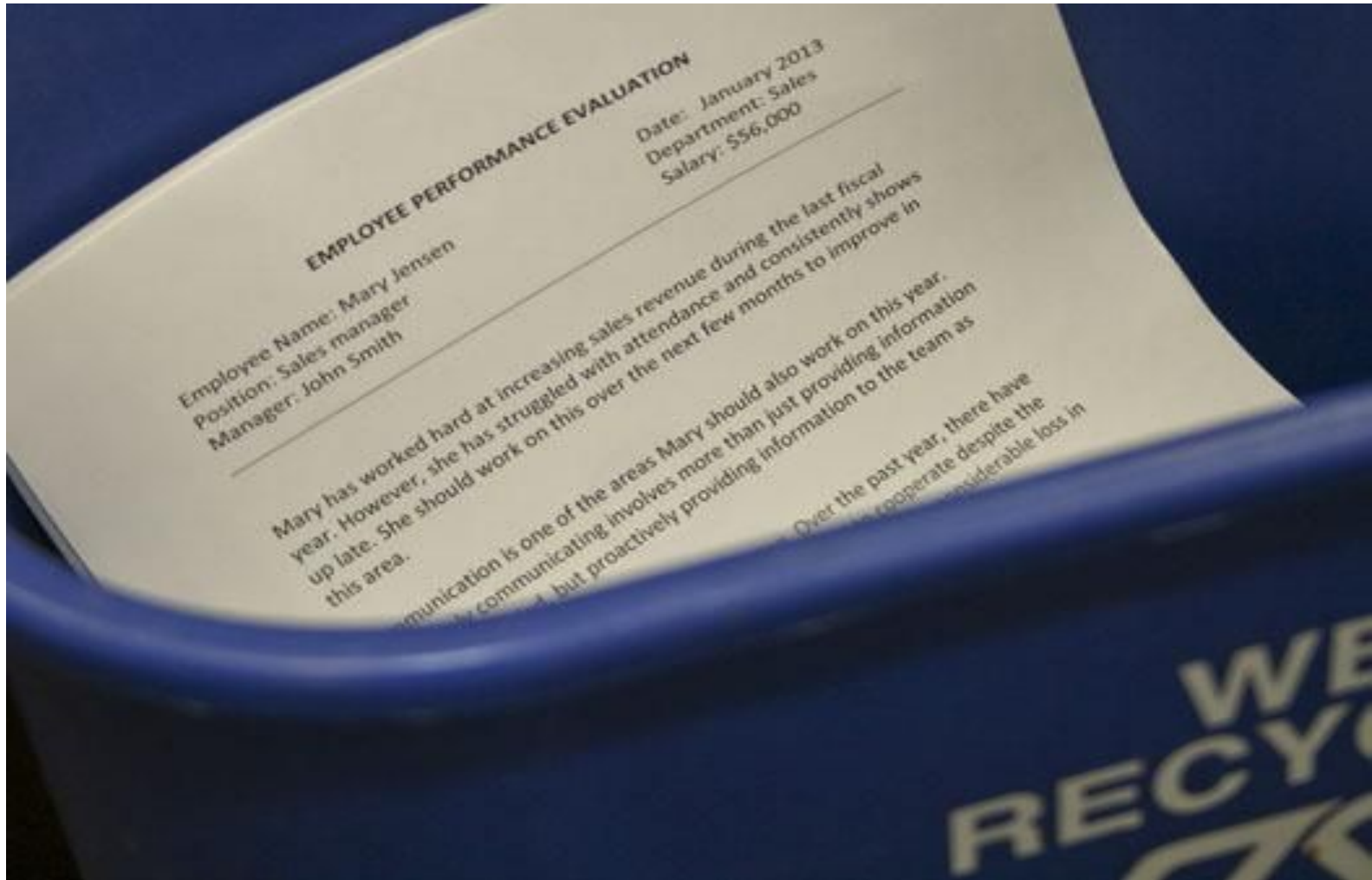


# Senhas e Exposição de Informações



# Descarte de Informações

FIAP



# **Mídias de Armazenamento Removíveis**

FIAP



# | Tailgating

FIAP





***“I heard they have seventeen cameras, twelve guards and a fingerprint scanners in their lobby. They say that place is like Fort Knox! Nobody can get in.”***

# Treinamento Inadequado

FIAP





# **Plano de Segurança Física e Ambiental**

# Plano de Segurança Física



- Busca a proteção de todos os ativos de uma organização;
- Inclui todas as instalações da organização;
- Deve contemplar também o transporte e destruição de tais ativos, incluindo mídias com informações confidenciais.
- Deve contemplar cuidados com o pessoal interno, externo e legislação vigente.
- Deve priorizar a vida humana.



- O Plano de Segurança Física deve tratar das ameaças ambientais: enchentes, terremotos, umidade, temperatura, ventilação, produtos químicos, etc.
- Localização geográfica das instalações trazem requisitos para o Plano de Segurança Física:
  - A organização pode ser alvo de protestos?
  - Existe histórico de falhas no fornecimento de serviços básicos?
  - A vizinhança oferece algum tipo de risco (instalações militares, empresas químicas, embaixadas)?
  - Fica próximo a grandes vias?

- Normas de Segurança do Trabalho
- Normas para Proteção Contra Incêndios
- Leis para Descarte de Material Perigoso
- Normas de Segurança da Informação