Os impactos da Lei Geral de Proteção de Dados na área da saúde

2º Congresso Nacional de Gestão em Saúde

UNIMED

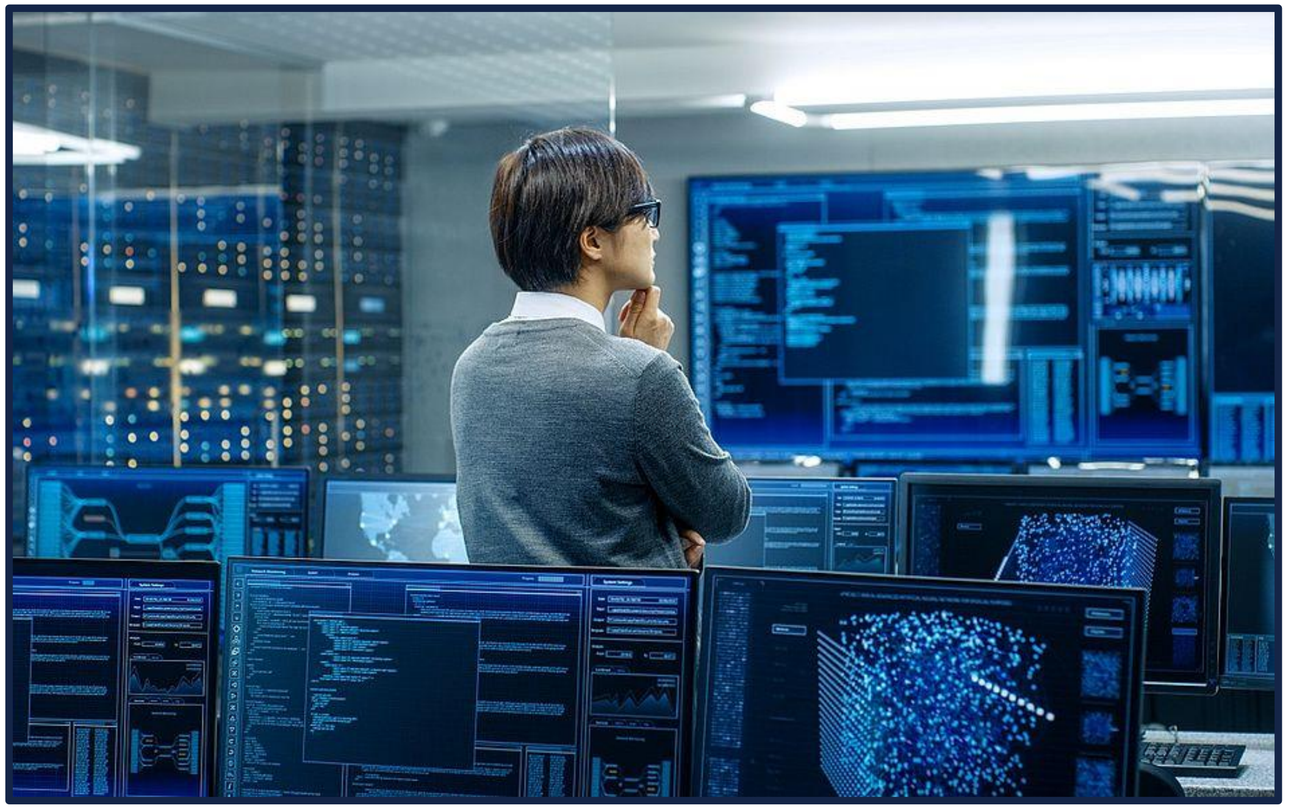
Domingo Montanaro

Domingo Montanaro

- Cofundador e CEO Ventura Enterprise Risk Management e Ventura Academy
- Perito em informática. 19 anos de experiência em elucidação de delitos praticados por meios eletrônicos
- Atuou na primeira condenação de “crime virtual” do Brasil (2004); bem como em mais de 200 prisões por cyber crime
- Co-fundou empresa de Inteligência Cibernética que logrou em 2017 selo de Empresa Estratégica de Defesa (EED) do Ministério da Defesa do Brasil
- Professor convidado da Poli-USP, Insper, FGV-SP, FGV-RJ, EPD e FAAP
- Treinou instituições governamentais (civis e militares) no Brasil, EUA, Emirados Árabes Unidos e Arábia Saudita
- Colaborador de órgãos públicos em diversas demandas, como *pro-bono*, desde 2001
- Integrante e contribuidor da HTCIA (High Technology Crime Investigation Association), APWG (Anti Phishing Working Group) e ICDF2C (International Conference on Digital Forensics and Cyber Crime)
- Pesquisador em Computer Forensics e Anti-Forensics. Palestrou em 16 países sobre suas pesquisas na área
- Fundador do São Paulo Cyber Crime Studies Group (Meetup mensal)

A “velha” economia e seus riscos

Transformação Digital

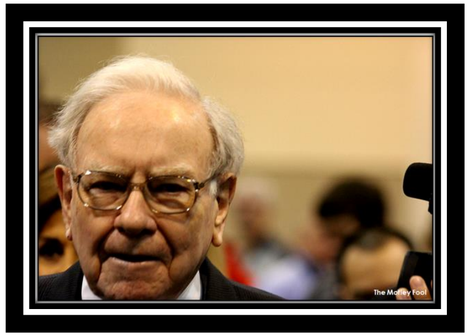


Investimento em TI levou as empresas de todos os setores da economia global à um novo patamar:

- **Alavancando vendas;**
- **Aumentando eficiência operacional;**
- **Proporcionando mais retorno ao acionista**

Bônus e Ônus

A conta chegou!



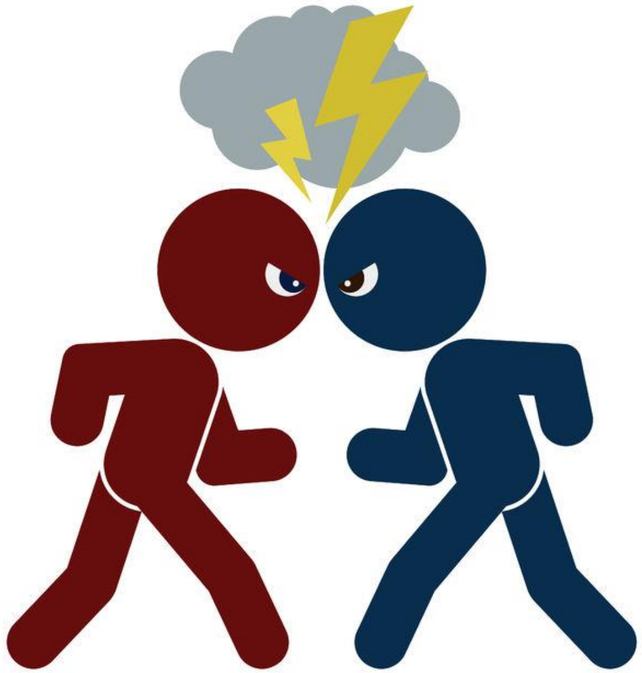
cyber, biological, nuclear or chemical attack

"...Our institutions are under cyber attack..."

Economic loss due to cybercrime is predicted to reach **$3 trillion by 2020**

VENTURA

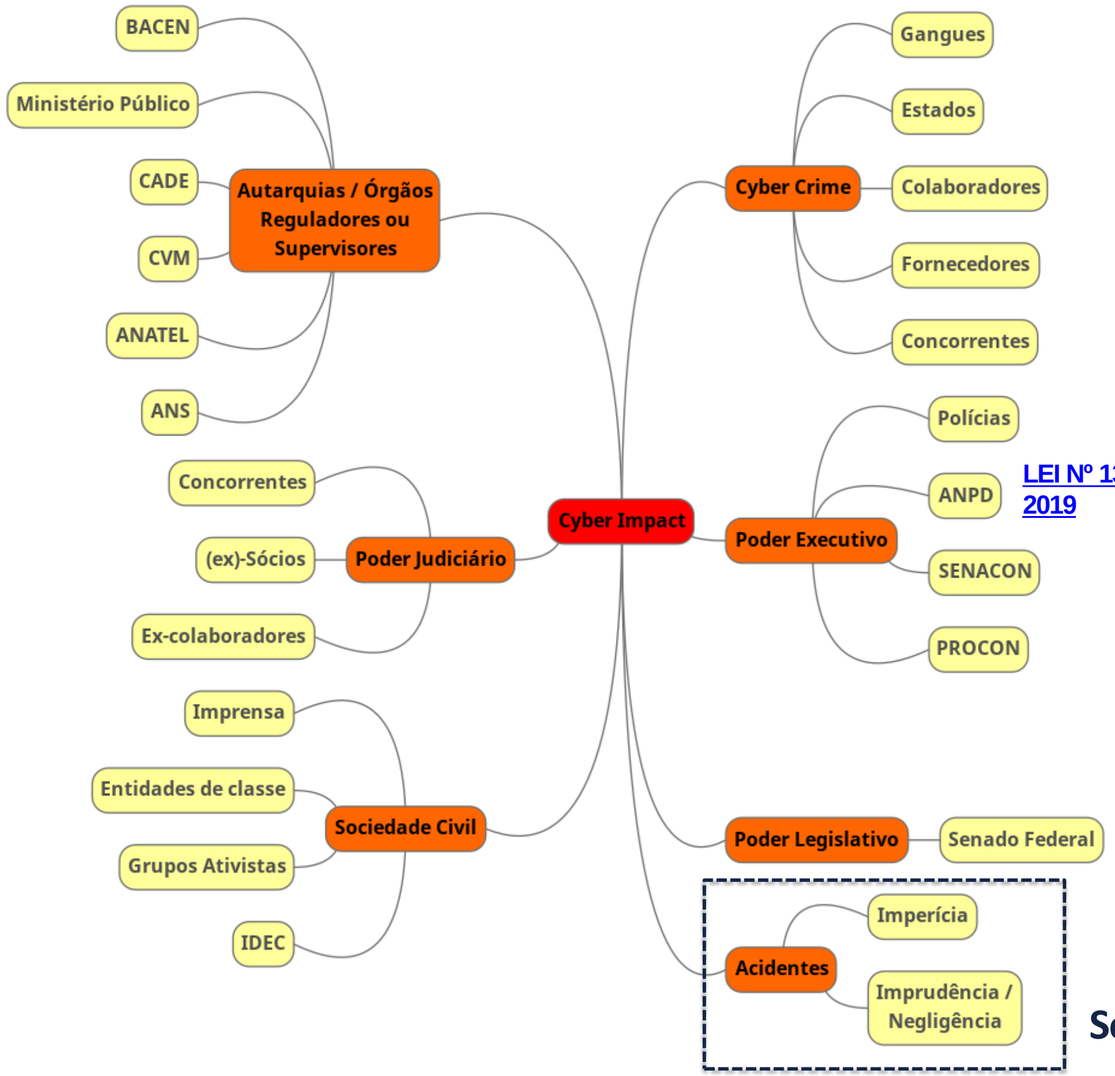
Quem é o adversário da sua instituição?



Adversário	Motivação
Gangue especializada	Financeira
Gangue amadora	Financeira
Ex-funcionário	Passional
Funcionário	Ideológica / Financeira / Passional / Concorrencial
Concorrente	Comercial
Exércitos (Estados)	Espionagem/PI
Ativista	Ideológica
Receitas (Estado)	Fiscalização
Polícias (Estado)	Investigação de delitos
Sócio	Concorrencial
Acionistas	Fiscalização
Script Kiddie	Curiosidade / Ego
Worms / Robôs	Coleção de ativos
Fornecedor	Financeira
Sindicato	Política
Órgão regulador	Fiscalização
Imprensa	Tração / Clientela

“Cyber Risk”

‘Cyber risk’ means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. (IRM)



[LEI Nº 13.853, DE 8 DE JULHO DE 2019]

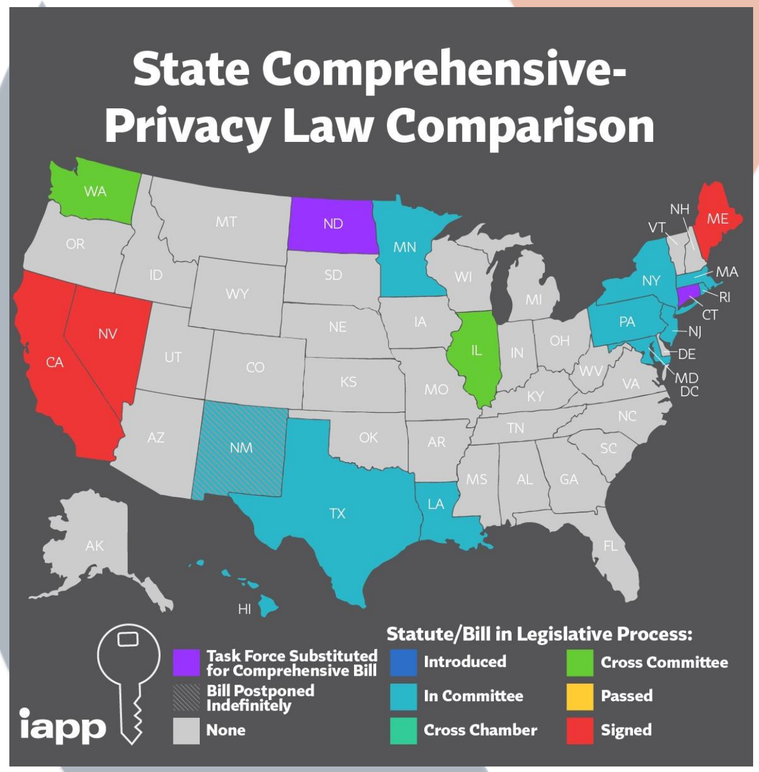
TI / Segurança

HIPAA
Health Insurance Portability & Accountability Act

1996

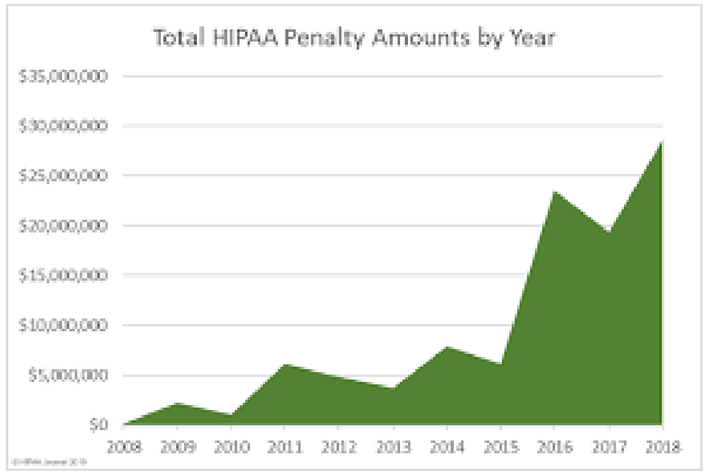
MAY 25TH 2018
GDPR

2018



2019

VENTURA



https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location
	Security Health Plan of Wisconsin, Inc.	WI	Health Plan	3657	07/19/2019	Hacking/IT Incident	Email
	Rockville Eye Surgery Center LLC dba Palisades Eye Surgery Center	MD	Healthcare Provider	2696	07/17/2019	Hacking/IT Incident	Email
	Northwood, Inc.	MI	Business Associate	583	07/16/2019	Unauthorized Access/Disclosure	Email
	Northwood, Inc.	MI	Business Associate	3881	07/16/2019	Unauthorized Access/Disclosure	Email
	Northwood, Inc	MI	Business Associate	5563	07/15/2019	Unauthorized Access/Disclosure	Email
	Wise Health System	TX	Healthcare Provider	35899	07/13/2019	Hacking/IT Incident	Email
	Northwood, Inc.	MI	Business Associate	5000	07/12/2019	Unauthorized Access/Disclosure	Email
	Rogerson House, Inc.	MA	Healthcare Provider	500	07/12/2019	Hacking/IT Incident	Network Server
	Cancer Treatment Centers of America (CTCA) at Eastern Regional Medical Center	PA	Healthcare	3904	07/12/2019	Hacking/IT Incident	Email

Medical Oncology Hematology Consultants, PA	DE	Healthcare Provider	8591	04/26/2019	Hacking/IT Incident	Email

(Displaying 1 - 100 of 509) 1 2 3 4 5 6 100

VENTURA

Observando o “tom” das autoridades globais

THE NETHERLANDS	Dutch Supervisory Authority for Data Protection (AP)	2019-06-18	460,000	Haga Hospital	Art. 32 GDPR	The Haga Hospital does not have a proper internal security of patient records in place. This is the conclusion of an investigation by the Dutch Data Protection Authority. This investigation followed when it appeared that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person. To force the hospital to improve the security of patient records, the AP simultaneously imposes an order subject to a penalty. If the Haga Hospital has not improved security before 2nd of October 2019, the hospital must pay 100,000 EUR every two weeks, with a maximum of 300,000 EUR. The Haga Hospital has meanwhile indicated to take measures.

http://www.enforcementtracker.com/

https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers

Publications

July 16, 2019

PDF Fine Decision Haga Hospital public version

DOWNLOAD

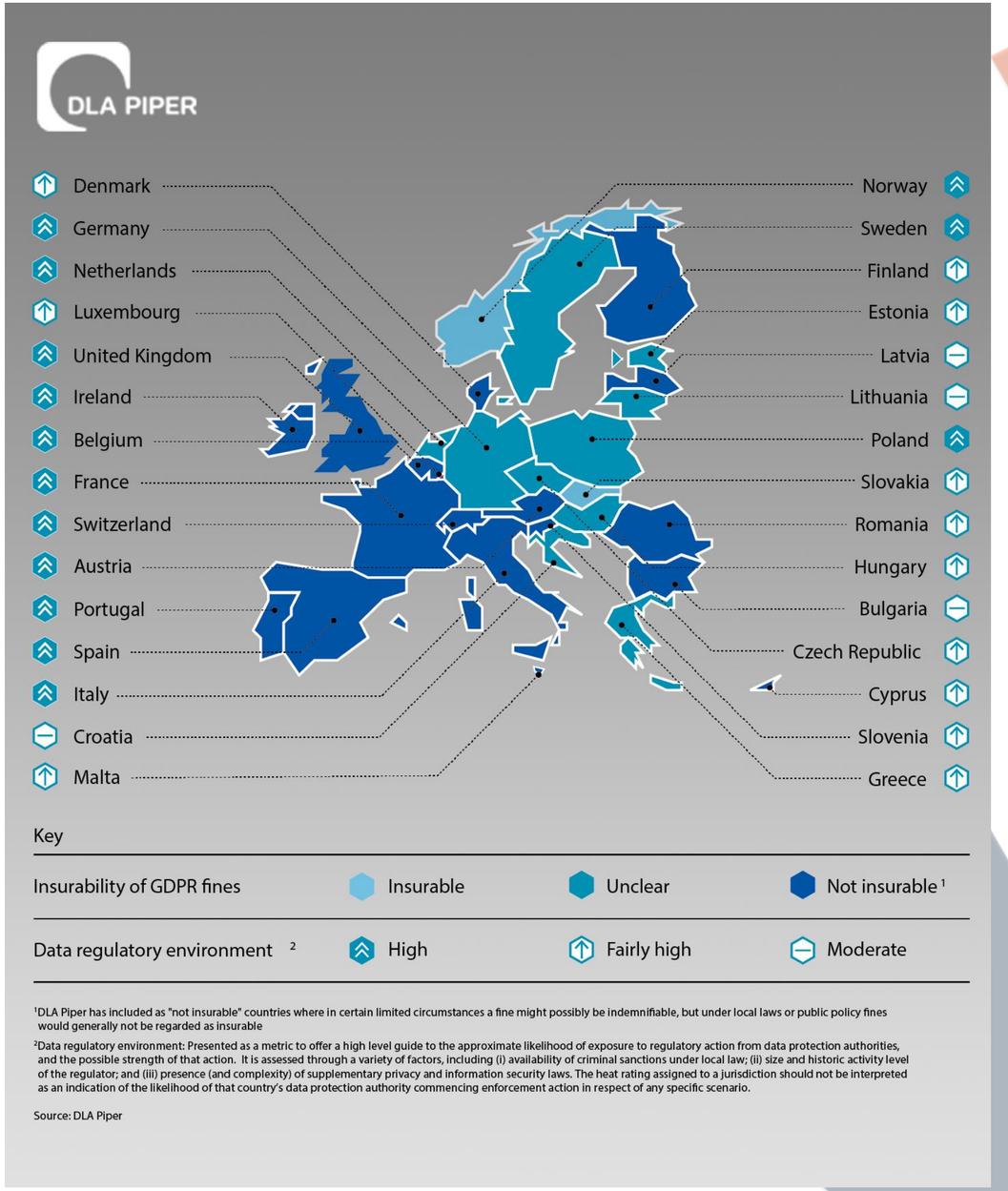
Report / July 16, 2019

PDF Research access digital patient records Haga Hospital

DOWNLOAD

VENTURA

Ah, mas eu tenho seguro!



http://img.response.aonunited.com/Web/AonUnited/%7B356f9069-b41d-4b70-94e3-359c5c7f74ed%7D_GDPR_DLA_Report_2nd_Edition_12_July_2019.pdf

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de **registros**, de **dados pessoais** ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os **direitos à privacidade**, à **proteção dos dados pessoais** e ao sigilo das comunicações privadas e dos registros.

...

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até **10% (dez por cento) do faturamento** do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - **suspensão temporária das atividades** que envolvam os atos previstos no art. 11; ou

IV - **proibição de exercício das atividades** que envolvam os atos previstos no art. 11.

Marco Civil da Internet – L12695 - 2014

ANPD

- Multa de 2% faturamento da empresa
- Limite de R$ 50MM

VENTURA

Centro Hospitalar Barreiro-Montijo

23 ABRIL 2018

Segurança dos dados clínicos dos doentes posta em causa

O Sindicato dos Médicos da Zona Sul (SMZS) tomou conhecimento de uma situação, a todos os títulos inaceitável, que coloca em causa a segurança dos dados clínicos de doentes tratados no Centro Hospitalar Barreiro-Montijo, contidos na aplicação informática utilizada para esse efeito.

O SMZS teve conhecimento que outros profissionais não médicos do Hospital acedem a essa aplicação com "perfil" médico, registando observações dos doentes como de um médico se tratasse.

Deste modo, estes profissionais não só passaram a ter acesso a TODA a informação médica, confidencial e que está protegida por segredo médico, como também ficam registados na aplicação como médicos, assumindo uma identidade e competências que não detêm.

Estes dados clínicos devem ser absolutamente confidenciais, são protegidos por normas legais e pelo segredo profissional médico. A garantia dessa confidencialidade está dependente do acesso por perfil médico e palavra-passe individuais, mecanismos de segurança que estão a ser ultrapassados.

O SMZS sabe que esta situação foi exposta ao Conselho de Administração, através do Diretor Clínico, que ainda não tomou qualquer posição relativamente a este assunto.

O SMZS considera que a situação em curso, ao comprometer a confidencialidade dos dados clínicos, representa um grave desrespeito pelos direitos dos doentes, configurando também uma inaceitável usurpação de perfis e prerrogativas médicas.

O acesso aos dados clínicos não pode ser facilitado. O SMZS considera que essa prática é ilegítima e ilegal, mesmo se determinada por medidas administrativas ou de gestão por parte da hierarquia.

Por esta razão, o SMZS decidiu fazer esta denúncia pública na defesa dos doentes e da segurança da sua informação, bem como da correcta identificação dos profissionais que os tratam.

O SMZS irá, como lhe compete, encaminhar para as entidades competentes os dados de que tem conhecimento, para que as responsabilidades sejam devidamente apuradas.

Lisboa, 23 de Abril de 2018

A Direção do Sindicato dos Médicos da Zona Sul (FNAM)

Em resposta a esta denúncia, o CHBM garante “que cumpre as regras de acesso ao sistema que contém os dados dos doentes e adverte que cabe a cada profissional de saúde não fornecer os seus dados a terceiros”. Assim, o Centro Hospitalar remete responsabilidades de eventuais falhas de segurança para os médicos.

Contactado pela Lusa, o centro hospitalar assegurou que apenas os médicos têm acesso ao ‘perfil médico’ no Sistema de Informação Clínico, a plataforma SClinico desenvolvida pelos Serviços Partilhados do Ministério da Saúde.

“Em nenhum momento é atribuído ‘perfil médico’ a profissionais não-médicos, pelo que o acesso através de perfil médico por profissional não-médico apenas é possível se o médico, contrariando todas as regras e normas de segurança, fornecer os seus dados de acesso a terceiros”, sublinha o CHBM numa resposta escrita enviada à Lusa.

O centro hospitalar explica que este sistema é acedido através da utilização de “nome de utilizador” + “palavra passe” específicos para cada utilizador, sendo a palavra passe definida pelo próprio utilizador de acordo com as regras de funcionamento do sistema.

30 ABRIL 2018

Administração confirmou acesso indevido a dados clínicos de doentes do Hospital Barreiro Montijo

O SMZS - Sindicato dos Médicos da Zona Sul denunciou recentemente a perda da segurança dos dados clínicos dos doentes internados no CHBM - Centro Hospitalar Barreiro Montijo por estes estarem a ser acedidos por profissionais não médicos através da utilização de um "perfil" médico na plataforma de registo SClinico.

Entretanto o Conselho de Administração (CA) dessa instituição veio contrapor que cumpre as regras em vigor e que o acesso à plataforma com perfil médico por profissional não médico apenas "é possível se o médico, contrariando todas as regras e normas de segurança, fornecer os seus dados de acesso a terceiros".

agentes da violação do seu dever de segredo e pondo em causa a confiança na relação médico / doente.

A versão contada à comunicação social pela administração do Centro Hospitalar Barreio / Montijo não tem, no entanto, qualquer sustentabilidade factual.

O SMZS sabe que são vários os perfis utilizados, de pelo menos duas especialidades médicas, e que essa utilização decorreu ao longo de vários meses, mesmo após o aviso ao CA que a situação estava a ocorrer. Durante este período, teria sido fácil identificar como teriam sido criados os dados de acesso de um perfil médico para um profissional não médico e terminar a utilização do perfil, se tivesse havido vontade de o fazer.

A opção, ao contrário, foi a da auto desculpabilização, não hesitando para tal em pôr em causa a confiança nos médicos da Instituição. O que apenas vem demonstrar a total incapacidade e irresponsabilidade do actual CA do CHBM.

O SMZS repudia por isso a tomada de posição do CA do CHBM e reafirma a sua intenção de promover o apuramento de todas as responsabilidades por esta situação intolerável.

06 JULHO 2018

Visita da OM ao Hospital Barreiro-Montijo para averiguar acesso irregular a dados clínicos

Na terça-feira, 3 de Julho, o Sindicato dos Médicos da Zona Sul (SMZS), representado por Guida da Ponte, acompanhou a visita do Bastonário da Ordem dos Médicos, Miguel Guimarães, ao Centro Hospitalar Barreiro-Montijo (CHBM), na sequência da denúncia do SMZS sobre o acesso irregular aos dados clínicos de doentes por profissionais não médicos nesse hospital.

A denúncia do SMZS, que foi feita em Abril deste ano, relatava que profissionais não médicos acediam à aplicação informática com um «perfil» médico, o que permitia ter acesso a toda a informação, confidencial e protegida por segredo médico, bem como ficar registado na aplicação como médicos.

Esta denúncia, fundamentada em factos, foi encaminhada para as autoridades competentes para a devida averiguação.

O Conselho de Administração do CHBM, confrontado com a denúncia pública da situação, afirmou que apenas cumpre as directrizes dos Serviços Partilhados do Ministério da Saúde (SPMS), desresponsabilizando-se por qualquer irregularidade .

O SMZS aguardará a averiguação dos factos, sendo certo que confirmando-se as ditas directrizes por parte da SPMS, organismo sob a tutela do Ministério da Saúde, este é responsável pela quebra da confidencialidade das informações clínicas dos doentes, e do segredo médico, o que acarreta graves implicações legais.

A Comissão Nacional de Protecção de Dados (CNPD) e a Inspecção-Geral das Actividades em Saúde vão investigar o caso de acesso irregular a dados clínicos no Hospital do Barreiro, que, segundo o bastonário dos Médicos, pode não ser caso único.

Numa visita realizada esta terça-feira ao Centro Hospitalar do Barreiro Montijo (CHBM), Miguel Guimarães sublinhou que acesso indevido de dados clínicos por profissionais não médicos denunciado naquela unidade "pode não ser caso único" e que vai alertar o Ministério da Saúde. O bastonário da Ordem dos Médicos salientou que a situação no Hospital do Barreiro "pode ser uma caixa de Pandora que vai mudar o nosso sistema todo", disse aos jornalistas.

O bastonário da Ordem dos Médicos espera que seja um processo rápido, até porque "a parte informática tem essa vantagem, é fácil perceber o que existe e se, no fundo, este sistema não está a funcionar".

Centro Hospitalar Barreiro-Montijo

- O Hospital do Barreiro tem 296 médicos colocados, mas os sistemas internos permitiam que mais de 900 médicos continuassem com as contas de acesso a repositórios clínicos ativa
- A deliberação revela ainda que, numa conta de teste, os peritos da CNPD conseguiram aceder a dados clínicos de um doente, que se encontravam nos arquivos digitais do Hospital de Santa Cruz, em Carnaxide
- O hospital não dispunha de regras internas para a criação de contas (que eram criadas depois do envio de e-mails pelos diferentes diretores dos serviços)
- Ou para os diferentes níveis de acesso à informação clínica.
- O método de autenticação não tinha em conta os dados identificativos que vinculam os diferentes profissionais ao hospital.

Tendo em conta o cenário que foi apurado numa primeira inspeção que remonta a julho, a deliberação da CNPD identificou **três infrações**: **violação do princípio da integridade e confidencialidade, violação do princípio da minimização de dados** que deveria impedir o acesso indiscriminado a dados clínicos dos doentes, **e incapacidade do responsável pelo tratamento dos dados para assegurar a confidencialidade e a integridade dos dados**. As duas primeiras infrações foram punidas com coima 150 mil euros cada, enquanto a terceira representou um acréscimo de 100 mil euros.

A CNPD realça a disponibilidade do Hospital do Barreiro para corrigir as diferentes falhas na gestão de acessos e repositórios clínicos, mas não deixa de considerar que a responsabilidade da unidade de saúde como «elevada», «**quanto à violação das restrições dos níveis de acesso dos profissionais aos dados pessoais dos clientes, uma vez que conscientemente permitiu associar o grupo funcional d**e "médico" **a quem apenas deveria estar credenciado com o perfil de** "técnico"».

A CNPD também responsabiliza a administração do Hospital do Barreiro por não ter tomado as medidas necessárias para garantir que as contas de médicos **que já não estavam a trabalhar no Barreiro eram** eliminadas.

Além de considerar que é «insustentável defender que qualquer assistente social possa aceder à totalidade do ficheiro clínico do cliente», a CNPD aponta o dedo à «**existência de credenciais de acesso que permitam a qualquer médico, de qualquer especialidade, a qualquer altura aceder aos dados dos clientes de um determinado centro hospitalar**».

A defesa do Hospital também lembrou que **a hierarquia dos perfis de utilizador e as políticas de acesso disponibilizadas pelas diferentes aplicações e repositórios clínicos são definidos por entidades terceiras (presumivelmente pela Serviços Partilhados do Ministério da Saúde (SPMS), que é responsável pelo braço tecnológico dos hospitais públicos). Além dos acordos de confidencialidade que abrangem todos os profissionais, o Hospital alega que as ferramentas informáticas disponibilizadas não permitiriam definir quem acede a que dados nos diferentes cenários.**

Pontuemos

Vulnerabilidade: **fraqueza de um ativo** ou de **um grupo de ativos** que **pode(m) ser explorada(s)** por uma ou mais **ameaças** (ISO 27001:2005)

Cenário clássico

Hmmm.. Vejamos:

<u>DPO pergunta para TI:</u>

Os dados dos clientes estão (pseudo) anonimizados?

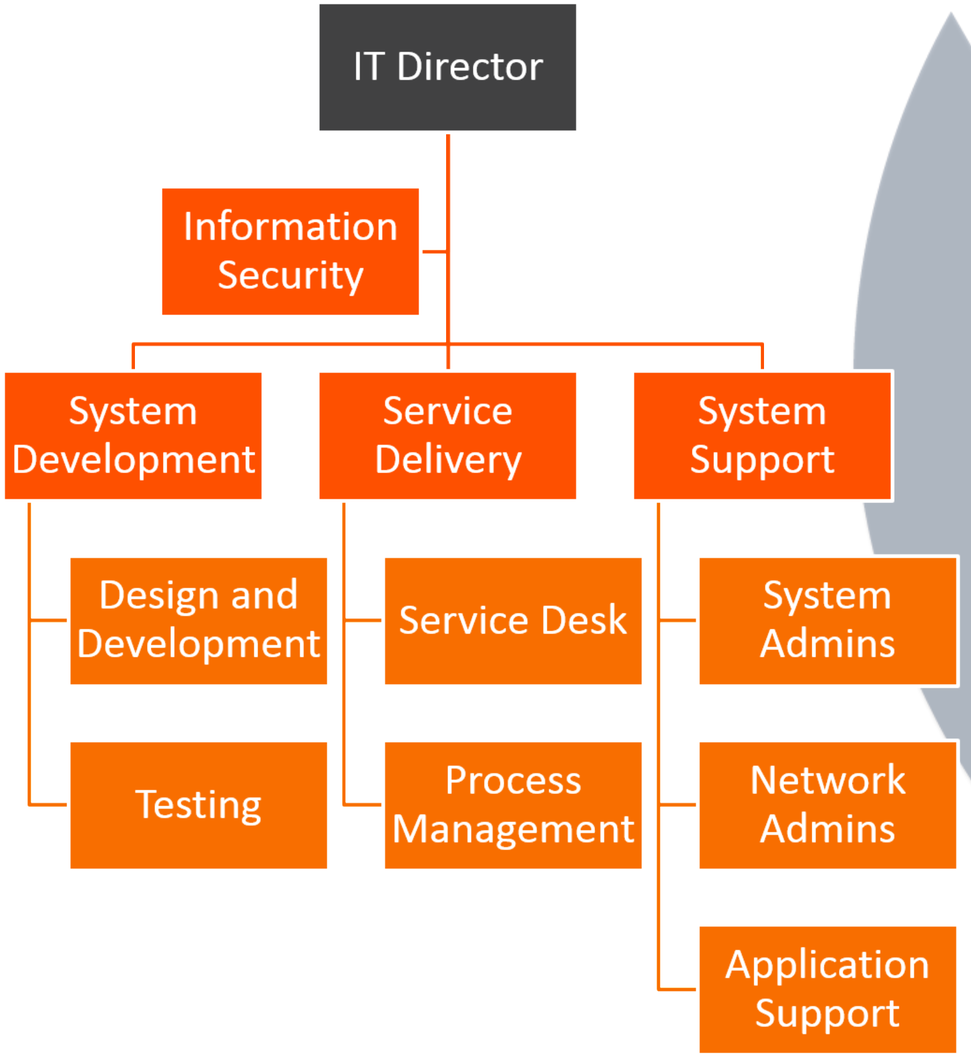
E dos pedidos (que podem conter dados pessoais)?

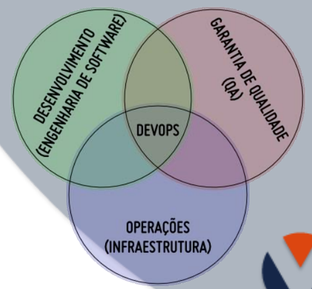
E das entregas?

Sim, claro!


How to Become an IT Project Manager
Job Path:
IT
Techie
Project Coordinator
Manager
Business Analyst
Non IT
Project Manager
What about Agile? Scrum? Other Certifications?
Job Description:
Job Skills
Job Path
Skills | Experience | Training
You Have
Gaps
Skills | Experience | Training
You Need
Plan
Training
PM = PM training dealing with technology - Infrastructure, Hardware, Software, Networks
ITIL = Information Technology Infrastructure Library = Best Practices used to develop & execute IT Service Management for the Company
ITSM = Information Technology Service Management = How You deliver of end to end IT services.

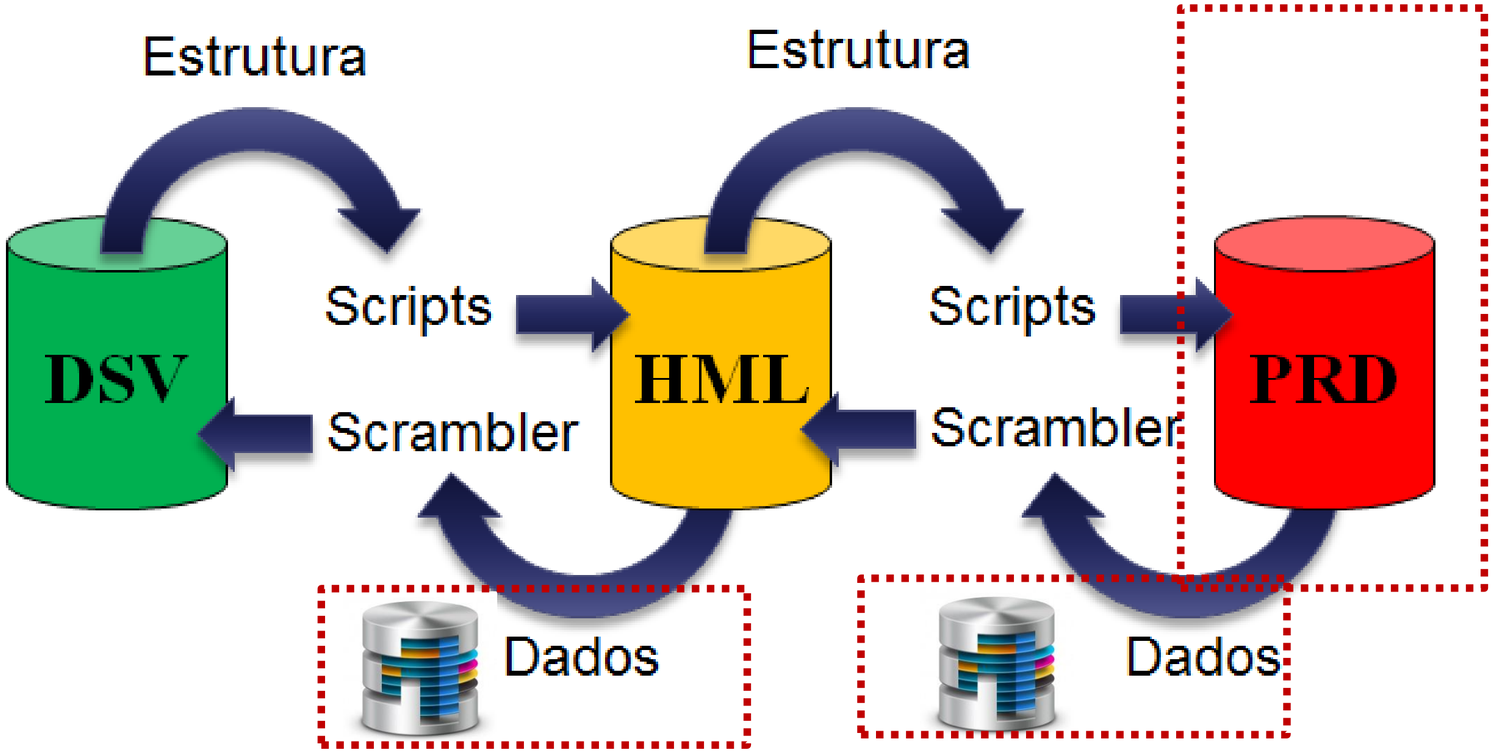
Perguntou à pessoa certa?





VENTURA

“Dentro da cozinha”



Foco das políticas de segurança.

Outras visões comumente esquecidas:

- Conciliação
  - 1234567890-R$150
- Debug
  - txtCC_1234567890 – 100ms
- Log
  - Cartão 1234567890 usado

VENTURA

Solução?

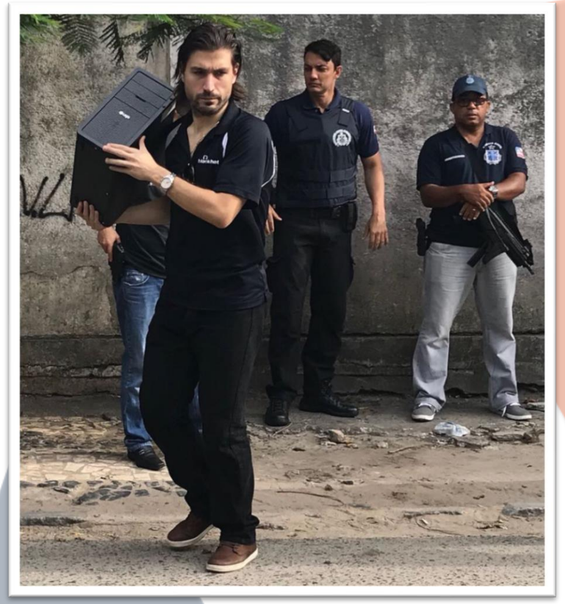
- Perícia!
- Metodologia: amostragem ou completa
- Se a inspeção pode ser feita por peritos, é bom se preparar utilizando profissionais à altura

Obrigado!

Domingo Montanaro
domingo@venturaERM.com

Cybercrime Studies Group

Grupo de estudos anti-cybercrime
Comunidade Brasileira
Reuniões na Av. Paulista
Próxima reunião: 30/07/2019
https://meetup.com/Sao-Paulo-Cybercrime-studies-group/



- ✓ **Capacitação de profissionais de TI e Jurídico**
- ✓ **Turmas presenciais e hands on**
- ✓ **Treinamentos criados a partir de casos reais**
- ✓ **Cursos in-company**