MetaRed Portugal | 17.nov.2021

Medidas de Proteção da **Informação**

Secundino Lopes
Departamento de Tecnologias, Escola Superior de Tecnologia e Gestão,
Instituto Politécnico de Portalegre, Portugal
secundino.lopes@ipportalegre.pt

Protocolo de Transferência de Hipertexto

HTTPS://www

Texto
Som
Vídeo
Imagem

Seguro

- Confidencialidade
- Integridade
- ~~Disponibilidade~~

Seguro

Confidencialidade

Autenticação

+

Encriptação

EnCt2514e7ea39fddc6290d3bc3addc53db5ec57dfc8f514e7ea39fddc6290d3bc3ad/0=ftyledgNiI7vggly1ypOssRa6P5ncyhgOFM+hjiQa3PITu1vAn+gtCU578dF4gk+iMRWJ6qJABHksnIfl6qjGONgjJNqbC407Z0V1k/vMA9DkdbDSorBz

Seguro

Confidencialidade

Encriptação

O método mais antigo de encriptação foi usado na Grécia antiga.

Seguro

Confidencialidade

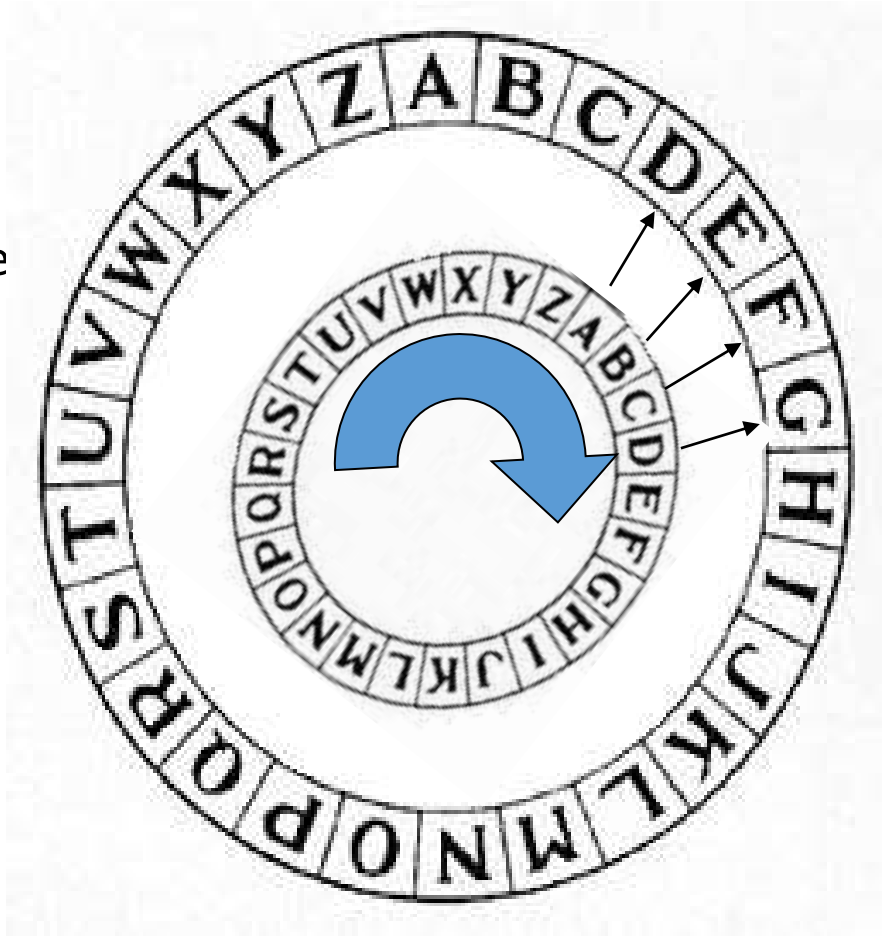
Encriptação

Caesar Cipher

Quando Júlio César enviava mensagens aos seus generais, ele não confiava nos mensageiros. Encriptava as mensagens substituindo cada letra:

- A com um D
- B com um E
- e assim por diante

Os generais conheciam a regra "<u>mudar por 3</u>" e podiam decifrar as mensagens.



Seguro

Confidencialidade

Encriptação

Vigenère Table
1586

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

F	L	A	N	K	E	A	S	T	A	T	T	A	C	K	A	T	D	A	W	N
S	E	C	R	E	T	K	E	Y	S	E	C	R	E	T	K	E	Y	S	E	C
X																				

Seguro

Confidencialidade

Encriptação

German Enigma Machine

Arthur Scherbius inventou a Enigma em 1918 e vendeu-a à Alemanha. Serviu de modelo para as máquinas usadas por todos os principais participantes da Segunda Guerra Mundial.

Estimou-se que, se 1.000 criptoanalistas testassem quatro chaves por minuto, todos os dias, seriam necessários 1,8 mil milhões de anos para experimentar todas as chaves possíveis.

Ciberespaço

O ambiente tecnológico criado pela interconexão mundial de equipamentos e serviços.

- ECOSSISTEMA de vida digital e **virtual** complexo …
- Espaço de liberdade sem fronteiras e sem controlo
- Alteração de comportamentos (**mentalidade de rebanho, tudo é viral, automutilação e suicídio, cyberbullying, …**)
- Novo espaço de conflito (cibercrime, cibersegurança, ciberterrorismo, ciber …) - nível de ameaça crescente
- "quinta dimensão" (terra, mar, ar, e espaço exterior) com influência económica, política, social e militar
- Preocupações de governabilidade

O que é *cibersegurança* ?

Segurança cibernética é um conjunto de técnicas que protegem as informações armazenadas nos computadores/smart devices que são transmitidas através das redes de comunicação, como a Internet.

Os ativos digitais são as informações confidenciais e essenciais ao negócio ou à pessoa, que possuem um determinado valor (estratégico) para a empresa/pessoa e devem, dessa forma, ser protegidos.

O que é que eu tenho que alguém pode querer ?

Dimensões da vida DIGITAL

SOCIAL PESSOAL

Redes Sociais (…), Rede dos CLIQUES
MOBILE | APP|Instant Messaging | Vídeo
Jogos|Apostas ONLINE

BYOD

ESTUDAR TRABALHAR

WWW, linkedin
Bibliotecas ONLINE | Wikipedia
Intranet|Proteção do Conhecimento

IA BigData IoT

CLOUD

COMPRAS ONLINE BANCOS

E-business
Setor Financeiro | Criptomoeda | BLOCKCHAIN
Amazon | FNAC | MB WAY | RFiD
Cartão Continente | Pingo Doce …
Seguros

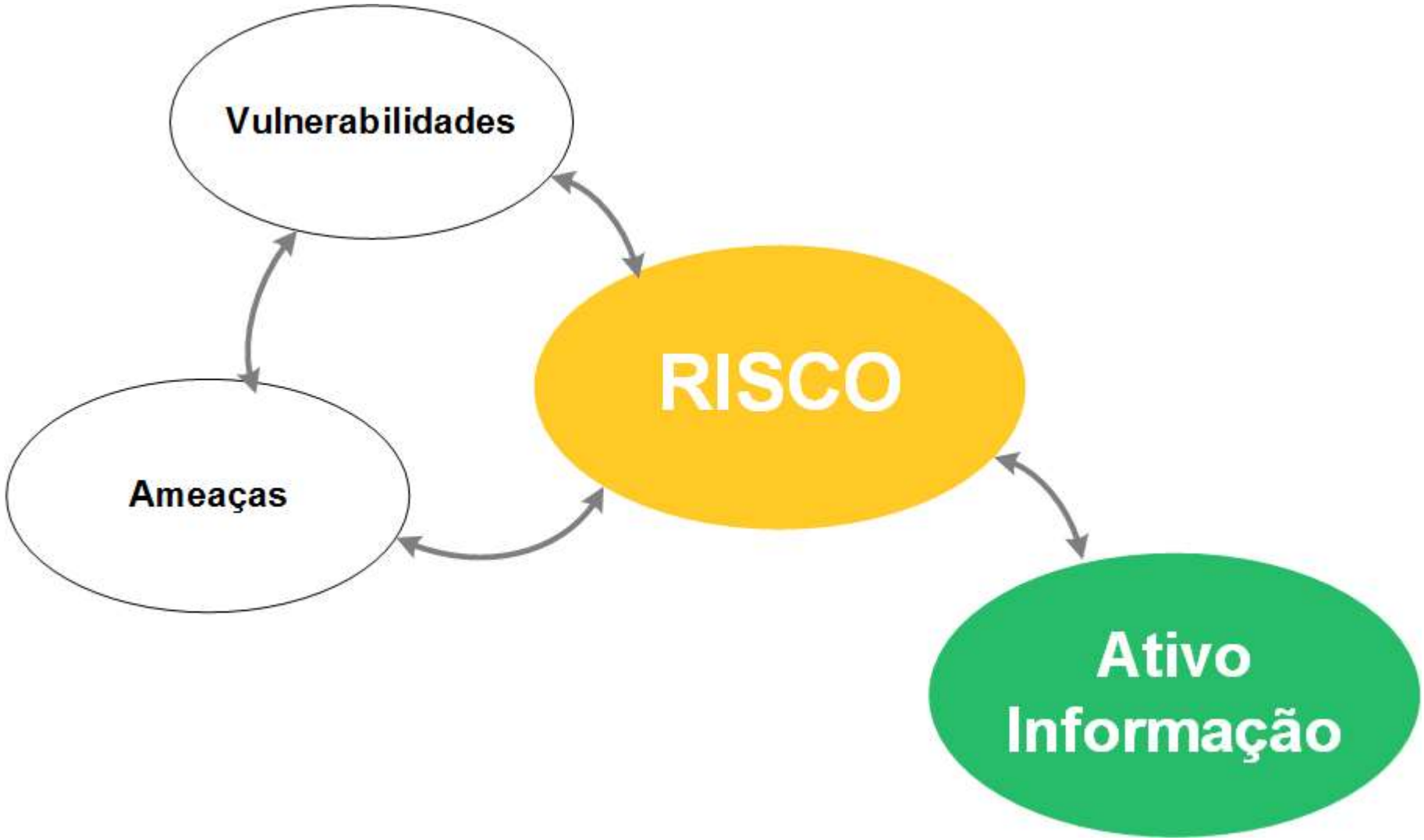
DADOS

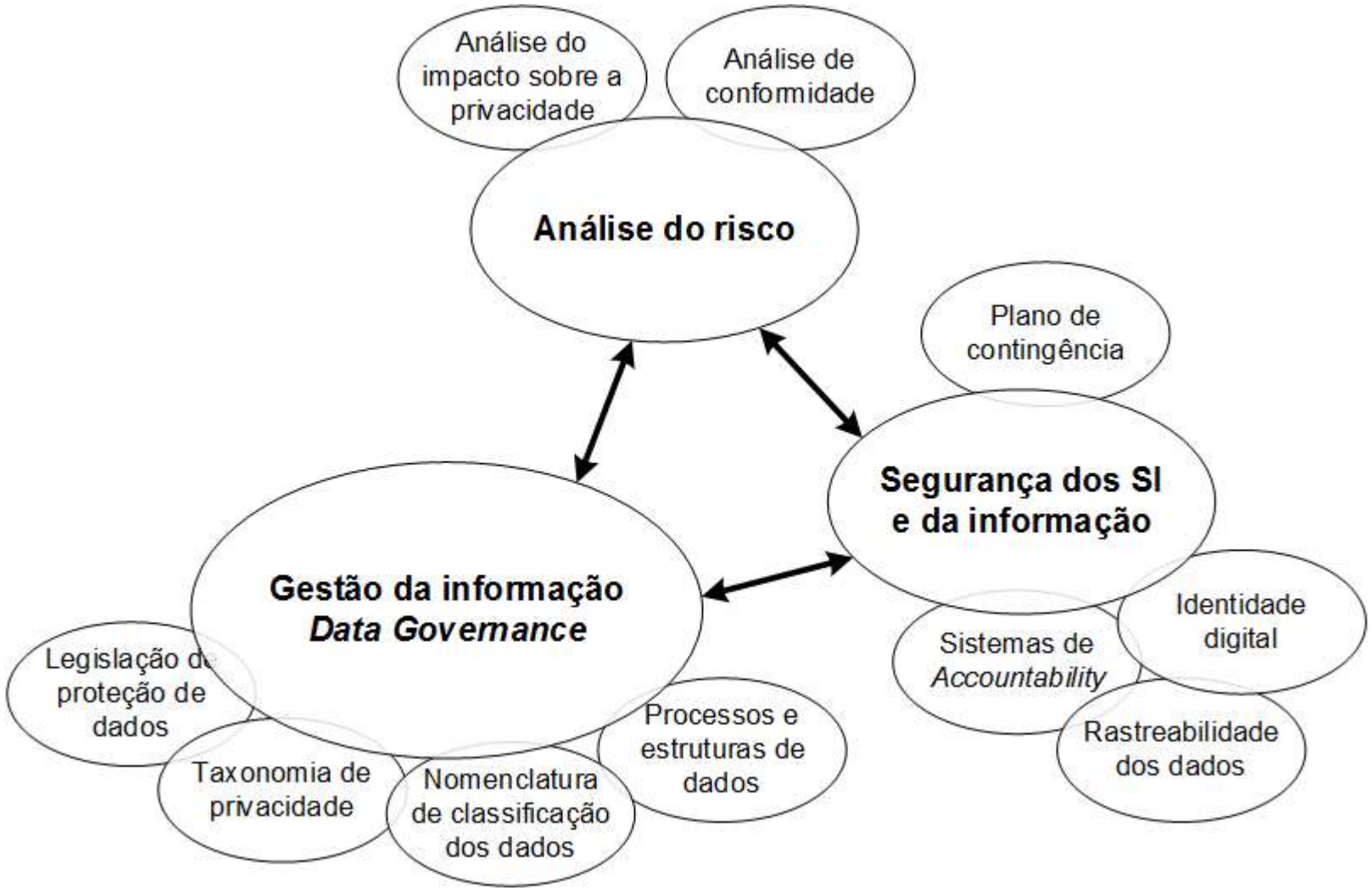
PÚBLICA ESTADO

Finanças
SNS
Segurança Social
CC|NIC + Passaporte
Áreas de Soberania

- Segurança adequada ao contexto da VIDA DIGITAL
- Aumentar as competências digitais → Aumenta a preparação em segurança
- Atuar de forma mais segura e informada
  - … a segurança é principalmente uma questão cultural e administrativa, e não técnica.
  - … a segurança não é apenas da responsabilidade de uma equipa dedicada ...
  - é necessário uma maior proximidade entre os especialistas em segurança e os utilizadores na prevenção de problema
  - competências em segurança são um desafio para a sustentabilidade das organizações


Proatividade
Colaboração
RISCO
Preparação
Capacidade


Vulnerabilidades
Ameaças
RISCO
Ativo
Informação


Análise do impacto sobre a privacidade
Análise de conformidade
Análise do risco
Plano de contingência
Segurança dos SI e da informação
Gestão da informação
Data Governance
Legislação de proteção de dados
Taxonomia de privacidade
Nomenclatura de classificação dos dados
Processos e estruturas de dados
Sistemas de Accountability
Identidade digital
Rastreabilidade dos dados

Segurança da Informação

Ideias !

1. BACKUPS regulares - INTEGRAR SO com CLOUD
2. Alterar palavra-passe com regularidade
3. Não utilizar email+password para autenticação
4. Esquemas de apropriação Identidade Digital
5. Verificar a origem dos emails e anexos !
6. Fazer "**log out**" de computadores partilhados
7. Partilhar o mínimo e de forma responsável !
8. Encriptar conteúdos de PENs, DISCOS
   BITLOCKER, DRIVE, ZIP, WORD