

## **PAINEL**

# ***“Garantias de Segurança para Cumprimento da Lei Geral de Proteção de Dados”***

## **ELBA VIEIRA**

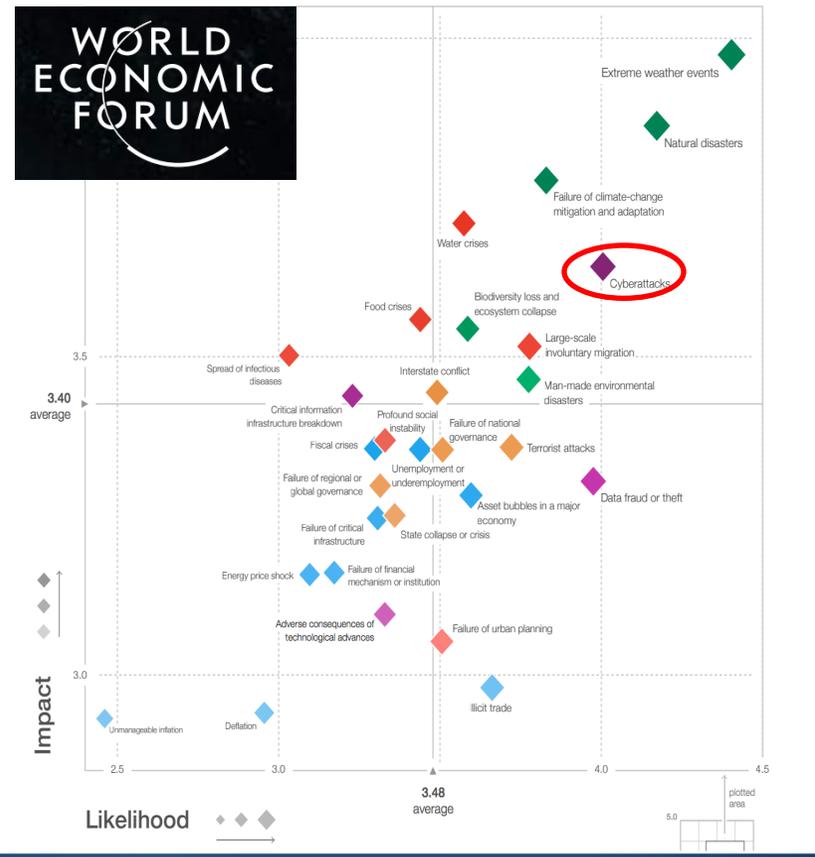
Consultora nas áreas de Segurança, Riscos e Tecnologia

Doutoranda em Ciência da Informação (UFBA)

LinkedIn: [linkedin.com/in/elba-vieira-03a0715](https://www.linkedin.com/in/elba-vieira-03a0715)



Figure I: The Global Risks Landscape 2018



Fonte: [http://www3.weforum.org/docs/WEF\\_GRR18\\_Report.pdf](http://www3.weforum.org/docs/WEF_GRR18_Report.pdf)

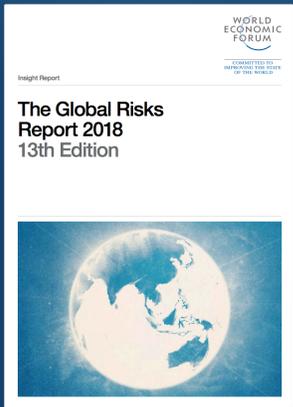
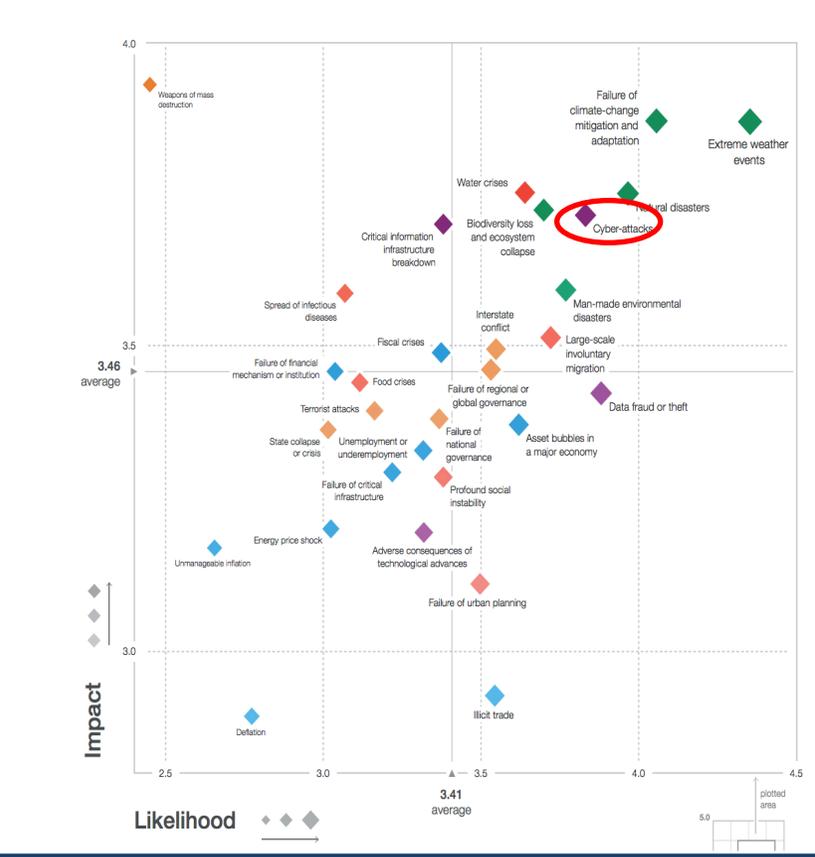


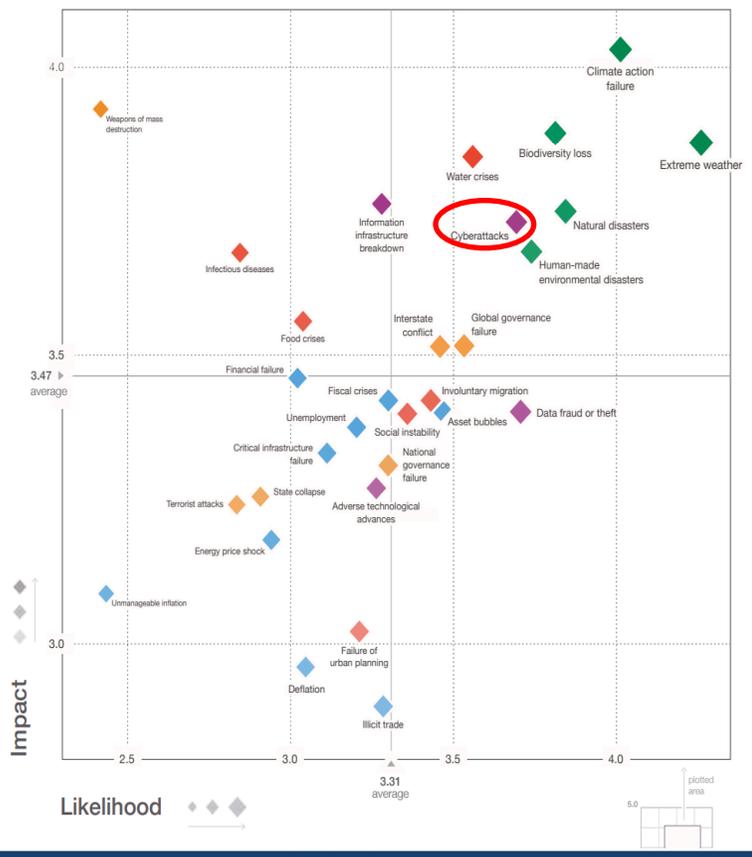
Figure I: The Global Risks Landscape 2019



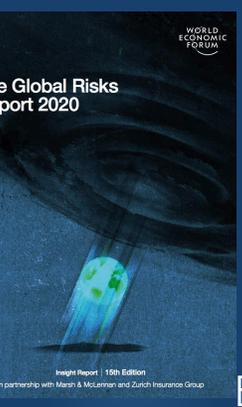
Fonte: [http://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2019.pdf](http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf)



Figure II: The Global Risks Landscape 2020



Fonte: [http://www3.weforum.org/docs/WEF\\_Global\\_Risk\\_Report\\_2020.pdf](http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)



# Risco

É a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, causando, dessa maneira, impactos e prejudicando a Organização.

*(NBR ISO/IEC 27005:2008)*

Segurança é uma prática voltada à eliminação de vulnerabilidades, para reduzir os riscos de uma ameaça se concretizar no ambiente que se quer proteger

# Segurança da Informação

- EDUCAÇÃO
- TREINAMENTO
- SENSIBILIZAÇÃO



- HARDWARES
- SOFTWARES
- MONITORAMENTO
- PROTEÇÃO

- POLÍTICAS
- NORMAS
- GUIAS
- DIRETRIZES

Fonte: [www.istockphoto.com](http://www.istockphoto.com)

ELBA VIEIRA



## DIÁRIO OFICIAL DA UNIÃO

Publicado em: 06/02/2020 | Edição: 26 | Seção: 1 | Página: 6  
Órgão: Atos do Poder Executivo

### DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020

Aprova a Estratégia Nacional de Segurança Cibernética.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, inciso VI, alínea "a", da Constituição,

#### DECRETA:

Art. 1º Fica aprovada a Estratégia Nacional de Segurança Cibernética - E-Ciber, conforme o disposto no inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018, na forma do Anexo a este Decreto.

BRASIL

CHILE



POLÍTICA NACIONAL DE CIBERSEGURIDAD

# ESTRATÉGIAS NACIONAIS DE SEGURANÇA CIBERNÉTICA

Fonte: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>

## ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

ESPAÑA



PORTUGAL

### ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

1. A Estratégia Nacional de Segurança do Ciberespaço, doravante designada por Estratégia, funda-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

2. A Estratégia assenta sobre os princípios gerais da soberania do Estado, das linhas gerais da Estratégia da União Europeia para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade, e alicerça-se nos seguintes cinco pilares:

Fonte: [https://www.ciberseguridad.gob.cl/media/2018/06/PNCS\\_Chile\\_ES\\_FEA.pdf](https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf)

Fonte: <https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019>

Fonte: [https://www.cncs.gov.pt/content/files/rcm\\_36-2015.pdf](https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf)

ELBA VIEIRA



11º SEMINÁRIO DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS

# Boas Práticas – Normas ISO – Família 27000

**ABNT ISO/IEC 27002:2013** - Código de prática para controles de segurança da informação

**ABNT ISO/IEC 27003:2017** - Sistemas de gestão da segurança da informação — Orientações

**ABNT ISO/IEC 27004:2016** - Monitoramento, medição, análise e avaliação

**ABNT ISO/IEC 27005:2019** - Gestão de riscos de segurança da informação

**ABNT ISO/IEC 27007:2018** - Diretrizes para auditoria de sistemas de gestão da SI

**ABNT ISO/IEC 27014:2013** - Governança de segurança da informação

**ABNT ISO/IEC 27017:2016** - Código de prática para controles de SI para serviços em nuvem

**ABNT ISO/IEC 27032:2015** - Diretrizes para segurança cibernética

**ABNT ISO/IEC 27701:2019** - Gestão da privacidade da informação

NIST Special Publication 800-53  
Revision 5

---

## Security and Privacy Controls for Information Systems and Organizations

---

JOINT TASK FORCE

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-53r5>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# CyBOK

## The Cyber Security Body of Knowledge

Version 1.0  
31<sup>st</sup> October 2019  
<https://www.cybok.org/>

### EDITORS

**Awais Rashid** | University of Bristol  
**Howard Chivers** | University of York  
**George Danezis** | University College London  
**Emil Lupu** | Imperial College London  
**Andrew Martin** | University of Oxford

### PROJECT MANAGER

**Yvonne Rigby** | University of Bristol

### PRODUCTION

**Joseph Hallett** | University of Bristol

Fonte: [https://www.cybok.org/media/downloads/CyBOK\\_version\\_1.0\\_YMKB7a.pdf](https://www.cybok.org/media/downloads/CyBOK_version_1.0_YMKB7a.pdf)

11º SEMINÁRIO DE  
PROTEÇÃO À PRIVACIDADE  
E AOS DADOS PESSOAIS

# Boas Práticas – Campanhas Educativas - ENISA



**Keep your password safe!**



**Working from a remote place?  
Do it safely!**



**...Don't make your  
organisation's confidential  
information available to everyone!**



## 10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



### Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.



### User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.



### Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.



### Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.



### Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



### Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

### Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.



### Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.



### Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.



### Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.



For more information go to [www.ncsc.gov.uk](http://www.ncsc.gov.uk) @ncsc

# Boas Práticas



Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil



Centro Nacional de Cibersegurança PORTUGAL



Equipo de Respuesta ante Incidentes de Seguridad Informática



Sistema Nacional de CIBERSEGURIDAD



National Institute of Standards and Technology  
U.S. Department of Commerce

11º SEMINÁRIO DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS

ELBA VIEIRA



# *Reflexões Finais*

**CRIAR** uma Cultura de Segurança da Informação

**GERENCIAR** riscos de segurança

**SENSIBILIZAR** pessoas em segurança e proteção de dados

**PROTEGER** infraestruturas críticas, dados pessoais e informações críticas

**ASSEGURAR** a privacidade de indivíduos (by Design e by Default)

# Obrigada!

*“Aponta pra fé e rema!!”  
(Los Hermanos)*

## ELBA VIEIRA

Consultora nas áreas de Segurança, Riscos e Tecnologia

Sócia-Fundadora da SOLARE Consultoria

Doutoranda em Ciência da Informação (UFBA)

Mestre em Gestão e Tecnologias Aplicadas à Educação (UNEB)

Coautora do livro “LGPD – Lei Geral de Proteção de Dados Pessoais /

Manual de Implementação” (Ed. Thomson Reuters)

LinkedIN: [linkedin.com/in/elba-vieira-03a0715](https://www.linkedin.com/in/elba-vieira-03a0715)



**Elba Vieira**

Doutoranda em Ciência da Informação |  
Consultora | Segurança | Riscos | Tecn...

