



Seminário do Curso de Produção Multimédia

Contextos profissionais do profissional em Produção Multimédia em Educação

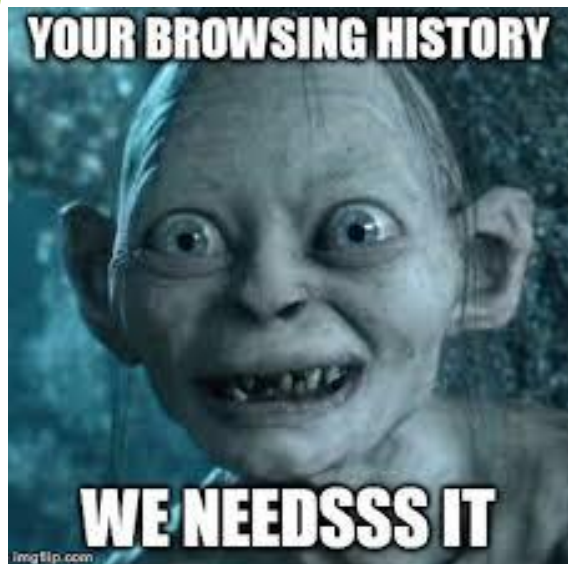
Papel e ética profissional

Proteção de dados

Princípios orientadores para os estudantes e professores do
Ensino Superior



it's your people, not your code, that makes the difference.....



Nobody Notices
What I do Until
I Don't Do It

“Um dos maiores desafios que os profissionais de TI de enfrentam é o de estar preparado e preparado para o inesperado. Especialmente estar preparado para responder a um incidente de segurança.”

Incidente de segurança

“ Um incidente de segurança é definido como qualquer **violação** inaceitável de uma **política, lei** ou como um **ato inaceitável** que envolva **dados, informação** ou **bens** como computadores, redes, comunicações, etc.”

Fonte: Sans Institute



Nobody Notices
What I do Until
I Don't Do It

Contextos profissionais do profissional em Produção Multimédia em Educação.
Papel e ética profissional.



Criar barreiras e pontos de controlo.

22 de fevereiro 2021

Nobody Notices
What I do Until
I Don't Do It

Contextos profissionais do profissional em Produção Multimédia em Educação.

Papel e ética profissional.



As equipas de segurança só controlam uma pequena parte do risco



Criar barreiras e pontos de controlo.



As barreiras são ultrapassáveis

Tratar o incidente



*Nobody Notices
What I do Until
I Don't Do It*

Contextos profissionais do profissional em Produção Multimédia em Educação.
Papel e ética profissional.



?

22 de fevereiro 2021

Nobody Notices
What I do Until
I Don't Do It



22 de fevereiro 2021

Nobody Notices
What I do Until
I Don't Do It



22 de fevereiro 2021

Nobody Notices
What I do Until
I Don't Do It

Um incidente de segurança vai ocorrer, só não se sabe quando.

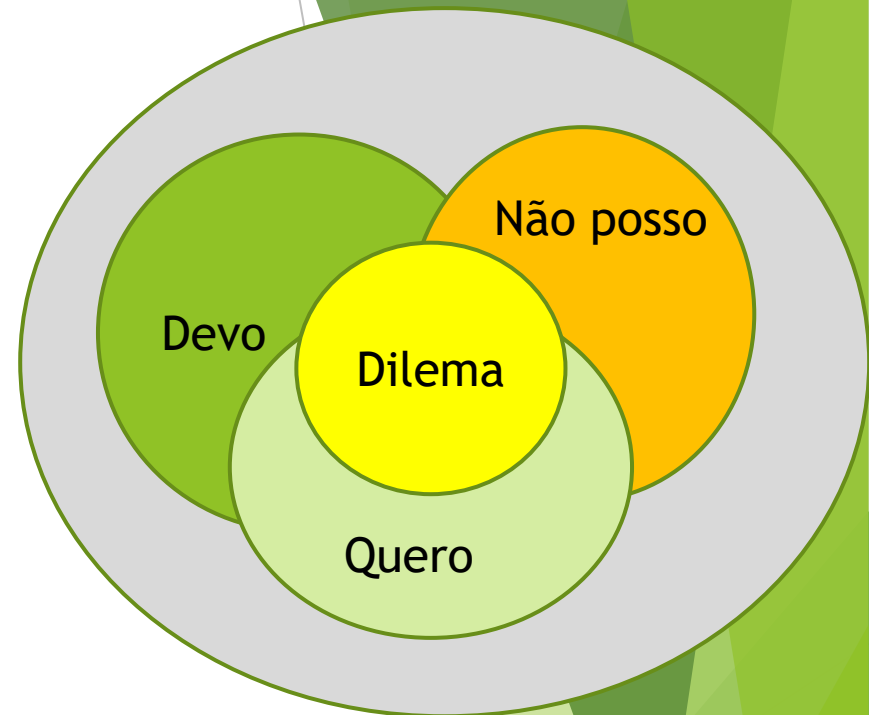
Ter a organização e equipas preparadas para a resposta a incidentes através do planeamento, comunicação e treino é essencial.





Requisitos das organizações:

- Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho de 27 de abril de 2016.
- **Lei 58/2019**, de 8 de agosto, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019.
- **Lei n.º 46/2018**, de 13 de agosto - Regime Jurídico de Segurança do Ciberespaço.
- **Resolução de Conselho de Ministros 41/2018**.
- **Diretiva (UE) 2016/1148** do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa à segurança das redes e da informação em toda a União (Network and Information Security Directive - NIS).
- **Estratégia Nacional de Segurança do Ciberespaço 2019-2023**.
- **Quadro Nacional de Referência para a Cibersegurança (QNRCS)**.



Nobody Notices
What I do Until
I Don't Do It

EPD/DPO – Encarregado de Proteção de Dados

- Não é uma posição nova, porém adquire relevância;
- Fundamental no cumprimento da RGPD ou Lei 58/2019;
- O ponto de contacto;
- Promotor/orquestrador;
- Nomeado por um Responsável ou Subcontratante;



RSI/CISO – Responsável pela Segurança da Informação

- Alinha a estratégia de segurança da informação com os objetivos da organização;
- Definir as normas de segurança e garantir seu cumprimento;
- Identificar a informação e processos críticos;
- Gerir os riscos de segurança da informação;
- Treinar e consciencializar;



Nobody Notices
What I do Until
I Don't Do It

Artigo 17.º

Direito ao apagamento dos dados («direito a ser esquecido»)

1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

- a) Os dados pessoais **deixaram de ser necessários para a finalidade** que motivou a sua recolha ou tratamento;
- b) O titular **retira o consentimento** em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º (Tratamento de categorias especiais de dados pessoais), n.º 2, alínea a) e **se não existir outro fundamento** jurídico para o referido tratamento;
- c) O titular **opõe-se ao tratamento** nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
- d) Os dados pessoais foram tratados **ilicitamente**;
- e) Os dados pessoais têm de ser apagados para o **cumprimento de uma obrigação jurídica** decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
- f) Os dados pessoais foram recolhidos no contexto da **oferta de serviços da sociedade da informação** referida no artigo 8.º, n.º1.

Artigo 24.º

Responsabilidade do responsável pelo tratamento

1. Tendo em conta a **natureza**, o **âmbito**, o **contexto** e as **finalidades do tratamento** dos dados, bem como os **riscos** para os direitos e liberdades das pessoas singulares, cuja **probabilidade** e **gravidade** podem ser variáveis, **o responsável pelo tratamento** aplica as **medidas técnicas e organizativas** que forem adequadas para **assegurar** e poder **comprovar** que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são **revistas** e **atualizadas** consoante as necessidades.

Artigo 32.º

Segurança do tratamento

1. Tendo em conta as **técnicas mais avançadas**, os **custos** de aplicação e a **natureza**, o **âmbito**, o **contexto** e as **finalidades** do tratamento, bem como os **riscos**, de **probabilidade** e **gravidade** variável, para os **direitos e liberdades** das **pessoas** singulares, o responsável pelo tratamento e o subcontratante aplicam as **medidas técnicas e organizativas** adequadas para assegurar um **nível de segurança** adequado ao **risco**, incluindo, consoante o que for adequado:

Artigo 32.º

Segurança do tratamento

(...)

- a) A **pseudonimização** e a **cifragem** dos dados pessoais;
- b) A capacidade de assegurar a **confidencialidade, integridade, disponibilidade e resiliência** permanentes dos **sistemas** e dos **serviços** de tratamento;
- c) A capacidade de **restabelecer a disponibilidade** e o acesso aos dados pessoais de forma atempada no caso de um **incidente físico ou técnico**;
- d) Um processo para **testar, apreciar e avaliar** regularmente a eficácia das **medidas técnicas e organizativas** para garantir a segurança do tratamento.

Artigo 25.º

Proteção de dados desde a conceção e por defeito

1. Tendo em conta as **técnicas mais avançadas**, os **custos** da sua aplicação, e a **natureza**, o **âmbito**, o **contexto** e as **finalidades** do tratamento dos dados, bem como os **riscos** decorrentes do tratamento para os **direitos e liberdades** das pessoas singulares, cuja **probabilidade e gravidade** podem ser **variáveis**, o responsável pelo tratamento **aplica**, tanto **no momento de definição** dos meios de tratamento como no **momento do próprio tratamento**, as **medidas técnicas e organizativas** adequadas, como a **pseudonimização**, destinadas a **aplicar com eficácia** os princípios da **proteção de dados**, tais como a **minimização**, e a incluir as **garantias** necessárias no tratamento, de uma forma que este **cumpra** os **requisitos** do presente regulamento e **proteja** os direitos dos titulares dos dados.

Artigo 35.º

Avaliação de impacto sobre a proteção de dados

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua **natureza, âmbito, contexto e finalidades**, for suscetível de implicar um **elevado risco** para os **direitos e liberdades das pessoas singulares**, o responsável pelo tratamento procede, **antes de iniciar o tratamento**, a uma **avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais**.

Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

Papel e ética profissional.

Normativos de apoio

ISO – 27001, 27005, 20000, 24760

ISO – 29134 (PIA)

CIS - Critical Security Controls

NIST - SP 800-100

Basic CIS Controls

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Assessment and Remediation
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational CIS Controls

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

Nobody Notices
What I do Until
I Don't Do It

Contextos profissionais do profissional em Produção Multimédia em Educação. Papel e ética profissional.

nau SEMPRE
A APRENDER



Consumidor Ciberseguro



RGPD para Implementadores na Administração Pública

nau SEMPRE
A APRENDER



Cidadão Ciberseguro



Introdução à segurança da informação classificada

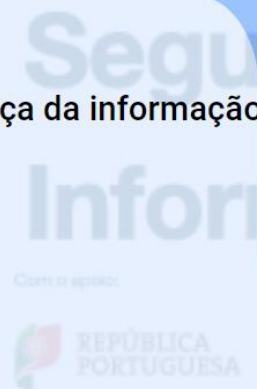


RGPD para Cidadãos Atentos

nau SEMPRE
A APRENDER




Cidadão Ciberinformado



Contextos profissionais do profissional em Produção Multimédia em Educação.
Papel e ética profissional.

MUITO OBRIGADO

?



Nobody Notices
What I do Until
I Don't Do It

Contacto: antonio.costa@cncs.gov.pt