Cibersegurança

CITECA

Webinar

04/02/2022

Início às 19h!

Início às 19h!

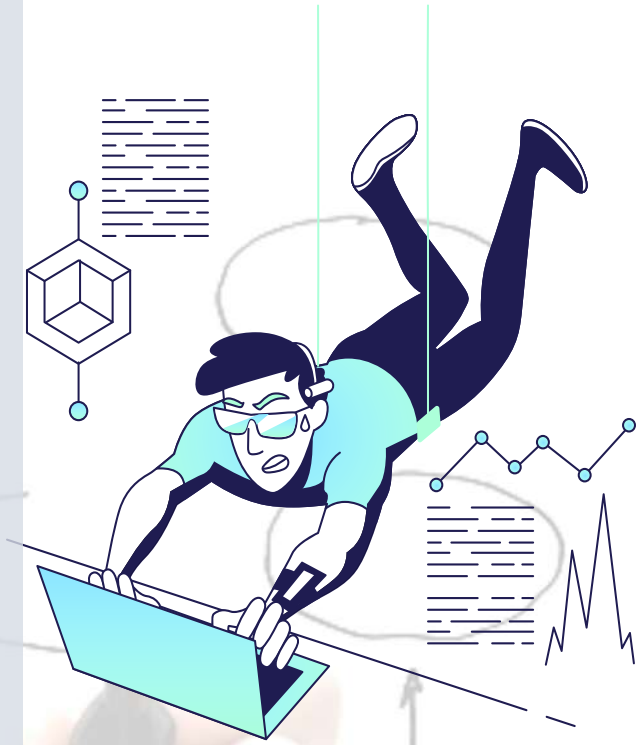
João Emílio Almeida
joaoalmeida@my.istec.pt

ISTEC Instituto Superior de Tecnologias Avançadas do Porto

Webinar – CIBERSEGURANÇA
ISTEC Porto / CITECA

Objetivos a atingir:

1. Compreender em que consiste a Cibersegurança
2. Saber quais são os riscos e as ameaças
3. Conhecer os tipos de ataques mais frequentes
4. Demonstração de algumas das ferramentas para testes de intrusão e deteção de vulnerabilidades (Kali Linux)
5. Enquadramento da responsabilidade legal pela salvaguarda e proteção dos dados (RGPD)
6. Ficar a conhecer planos de resposta ao incidente, recuperação de dados e retoma da normalidade



Webinar – CIBERSEGURANÇA
ISTEC Porto / CITECA

Resumo da apresentação:

1. Enquadramento
2. Riscos e ameaças
3. Tipos de ataques mais comuns
4. Demonstração de ferramentas para teste de vulnerabilidades
5. Enquadramento legal (RGPD)
6. Gestão do incidente: comunicação, equipas de intervenção

BREVE APRESENTAÇÃO...

- CV académico:
  - Curso Complementar de Electrotecnia (Fontes Pereira de Melo) 1982-84
  - Bacharelato Eng. Informática – ISEP 1985-88
  - Eng.Informática Industrial (licenciatura) – ISEP 1992/5
  - Frequência Mestrados em Ciências da Computação (FCUP) e Inteligência Artificial (UP – FEUP, FCUP, FEP)
  - Mestrado em Segurança Contra Incêndios Urbanos, 2005/7, DEC-FCTUC Univ. Coimbra / LNEC
  - Doutoramento Engª Informática (FEUP 2016)
  - Pós-graduação em Virtualização e Cloud-Computing
- CV profissional:
  - Resp. Sistemas Informação – Emílio de Almeida – Desp. Oficial, Lda 1984-95
  - Analista de Sistemas / Programador Sénior – Real Vida Seguros, S.A. 1988-2003
  - Diretor Técnico – AVANTEC – Tecnologias Avançadas, Lda 2000-2011
  - Docente Ensino Superior – FEUP, IPCA, ISTEC 2017-
  - ISTEC Porto:
    - Presidente do Conselho Técnico-Científico
    - Diretor curso Licenciatura em Engenharia Informática
    - Coordenador do CTeSP Redes e Sistemas Informáticos
    - Diretor do CITECA – Centro de Investigação e Tecnologias Avançadas

ISTEC Instituto Superior de Tecnologias Avançadas do Porto

ISTEC Porto | www.istec-porto.pt

Cursos

Licenciaturas

CTeSP Cursos Técnicos Superiores Profissionais

PG Pós-Graduações

Finalidade:

- Ensino superior na área das **tecnologias da informação e multimédia**
- Transferência e valorização do conhecimento científico
- Desenvolvimento profissional de alto nível
- Protocolos de colaboração com instituições de ensino superior nacionais e estrangeiras

Projeto Educativo:

- **Ensino Superior** nos domínios da **Informática, Multimédia, Redes e Telecomunicações e Cibersegurança**
- **Formação Pós-graduada**, formação especializada e contínua na área das **Tecnologias de Informação e Comunicação (TIC)**
- Utilização de tecnologias pedagógicas da multimédia interativa e dos sistemas de comunicação e de interação on-line, tendo como objetivo maximizar a eficiência do ensino e da aprendizagem
- **Investigação orientada** para projetos de âmbito nacional e internacional que envolvam desenvolvimento profissional de alto nível tecnológico
- Estabelecimento de uma **rede privilegiada de parcerias** com instituições de ensino superior, empresas, instituições públicas e associações da sociedade civil no Porto e no Norte, de forma a criar sinergias que sejam vantajosas e competitivas para a afirmação do Instituto, quer no plano nacional, quer no plano internacional.

RISCO CIBERNÉTICO – O que é?

"O conceito de Cibersegurança, ao longo dos tempos, até motivado pela própria noção de transformação digital, tem sido alvo de diversas interpretações. Se pode ser entendido como **o conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação**, pode, por outro lado, ser definido como **o sentimento de segurança percecionado pelas pessoas quando usam a Internet e as tecnologias digitais**."

In CNCS - https://www.cncs.gov.pt/pt/sobre-nos/#oquee

RISCO CIBERNÉTICO – Factos

1967 – 1º relatório sobre segurança

1988 – primeiro virus para PC: Morris

2013/14 – JPMorgan Chase: 40M CC e 70M e-mails

2013/14 – Yahoo: 3B users

2015 – OPM 21,5M SF-86 clearance data

2016 – Facebook, IRA e Cambridge Analytica (eleições presidenciais EUA)

2017 – Equifax (USA consumer credit company, Atlanta)

2017 – WannaCry Ransom attack

2018 – VPN Filter Cyber attack MITM (500.000 routers)

2019 – FB e passwords; 267M pass à venda dark web

2020 – Marriott Hotels 500M users data leak

RISCO CIBERNÉTICO – Factos

2020 – COVID-19 pandemic; zoom

2020 – custos mundiais de 124 USD biliões (mil milhões) com aumento 8,7% dos custos ao ano

2025 – Allianz estima prémios de US$20 Billions (4 em 2020)

RISCO CIBERNÉTICO – Trends

- **Falta de recursos**: humanos e financeiros
- **Falta formação**: técnicos especializados e colaboradores em geral
- **Segurança**: última prioridade
- **Weak applications**: desenvolvimento sem testes adequados e foco na segurança
- **Weak networks**: falta de planeamento e testes
- **Complexidade**: incremento no número equipamentos, software, aplicações, sistemas…
- **Visibilidade da Segurança**: ou invisibilidade da insegurança…
- **Cloud: assumir** que é mais seguro e permite relaxar na segurança
- **Aprender com erros do passado**

RISCO CIBERNÉTICO – Factos em PT

E em Portugal?

Dados de 2020

- 55% aumento tráfego dados (ANACOM)
- 4% + agregados familiaress ligados internet
- 3% + utilizadores internet (INE)
- 40% utilizadores em confinamento (INE)
- 39% exposição à desinformação (eurobarómetro)
- 64% CM têm estratégia seg.informação
- 78% CM necessitam reforço eq.inf.

https://www.cncs.gov.pt/docs/relatorio-sociedade2021-observ-cncs.pdf

Formação em Cibersegurança em PT

Cursos de Especialização Tecnológica de Cibersegurança e Segurança de Informação, divulgados pela DGES, em Portugal, 2021

Formação	Instituição
Cibersegurança	ATEC – Associação de Formação para a Indústria
Cibersegurança	Centro de Emprego e Formação Profissional de Coimbra
Cibersegurança (NOVO)	Centro de Emprego e Formação Profissional do Médio Tejo
Cibersegurança	Instituto Profissional de Tecnologias Avançadas para a Formação, Lda.
Cibersegurança (9 cursos)	NOVOTECNA – Associação para o Desenvolvimento Tecnológico

Tabela 6 | DGES (recolha CNCS)

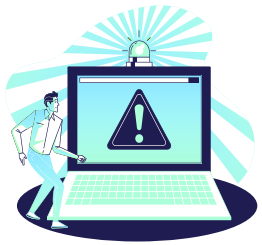
Formação em Cibersegurança em PT

Cursos superiores de cibersegurança e segurança de informação registados pela DGES, em Portugal, 2021

Formação	Tipo/Grau	Instituição
Cibersegurança	TESP	Instituto Politécnico da Guarda – Escola Superior de Tecnologia e Gestão
Cibersegurança	TESP	Instituto Politécnico da Lusofonia – Escola Superior de Engenharia e Tecnologias
Cibersegurança	TESP	Instituto Politécnico de Bragança – Escola Superior de Tecnologia e de Gestão de Bragança
Cibersegurança (NOVO)	TESP	Instituto Superior de Tecnologias Avançadas de Lisboa
Cibersegurança e Redes informáticas (NOVO)	TESP	Instituto Politécnico de Leiria – Escola Superior de Tecnologia e Gestão
Cibersegurança, Redes e Sistemas Informáticos	TESP	Instituto Politécnico do Porto – Escola Superior de Tecnologia e Gestão
Cibersegurança, Redes e Sistemas Informáticos	TESP	Instituto Politécnico Jean Piaget do Sul – Escola Superior de Tecnologia e Gestão Jean Piaget
Redes e Segurança Informática	TESP	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior
Segurança e Proteção de Dados para Sistemas de Informação (NOVO)	TESP	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior
Segurança Informática em Redes de Computadores	Licenciatura	Instituto Politécnico do Porto – Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Instituto Politécnico de Viana do Castelo – Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Universidade de Aveiro
Cibersegurança e Auditoria de Sistemas Informáticos (NOVO)	Mestrado	Instituto Superior Politécnico Gaya
Cibersegurança e Informática Forense	Mestrado	Instituto Politécnico de Leiria – Escola Superior de Tecnologia e Gestão
Engenharia de Segurança Informática	Mestrado	Instituto Politécnico de Beja – Escola Superior de Tecnologia e de Gestão
Segurança de Informação e Direito no Ciberespaço	Mestrado	Universidade de Lisboa – Faculdade de Direito e Instituto Superior Técnico; com Instituto Universitário Militar – Escola Naval
Segurança Informática	Mestrado	Universidade de Coimbra – Faculdade de Ciências e Tecnologia
Segurança Informática	Mestrado	Universidade de Lisboa – Faculdade de Ciências
Segurança Informática	Mestrado	Universidade do Porto – Faculdade de Ciências
Segurança de Informação	Doutoramento	Universidade de Lisboa – Instituto Superior Técnico

Pós–Graduação: CiberSegurança e Incidentes Cibernéticos

- **Em parceria com o ISTEC-Porto / DefendeRisk Academy / CIIWA**
- **Corpo Docente altamente especializado**
- **Horário pós-laboral:** Ensino híbrido (presencial e à distância);
- **Destinatários:** empresários, administradores, diretores, gestores e quadros superiores de organizações privadas e públicas




A **DefendeRisk Consultores** surgiu em 2018 na **Maia**.

Presta serviços na área da **Gestão Integral dos Riscos Patrimoniais e Formação especializada**.

A **DefendeRisk Academy** já vai na 3ª edição da Pós-Graduação em "Risk Management em Peritagem de Sinistros", na Coimbra Business School / ISCAC, em parceria com a DefendeRisk Consultores e com a GEP, Gestão de Peritagens S.A..

Público-alvo:
- Peritos ou candidatos a essa profissão
- Gestores de Sinistros
- Gestores de Risco
- Quadros de Seguradores nacionais e do universo da CPLP (Comunidade de Países de Língua Portuguesa).

Coordenação da PG:
- Dra. Guilhermina Freitas, ISCAC
- Eng. Lúcio Pereira da Silva, DefendeRisk Consultores
- Dr. Vasco Martins Pereira, GEP, Gestão de Peritagens, S.A.

DefendeRisk®
Consulting & Technical Audits

A **Competitive Intelligence & Information Warfare Association (CIIWA)** é uma associação civil, sem fins lucrativos, cujo objetivo primordial é o desenvolvimento de uma comunidade internacional e de uma rede de conhecimento entre entidades, especialistas e demais interessados na temática da Competitive Intelligence e da Guerra de Informação.

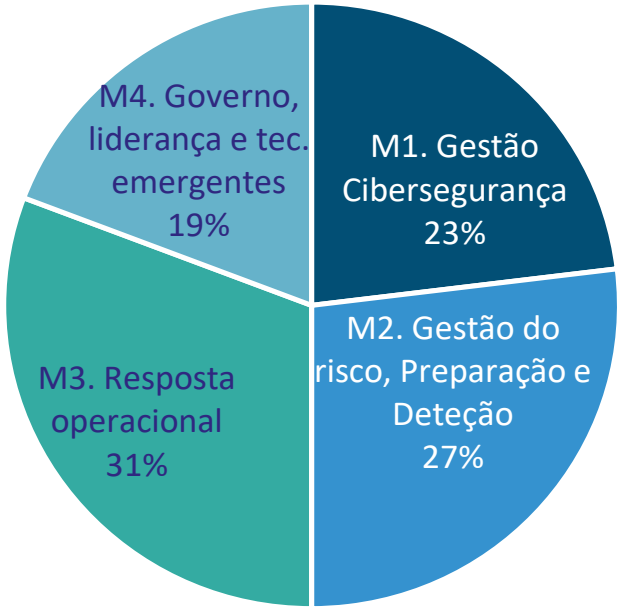
Nasceu no meio académico, a partir de uma iniciativa dos Alunos do Curso de Pós-Graduação em Guerra de Informação / *Competitive Intelligence* da Academia Militar.

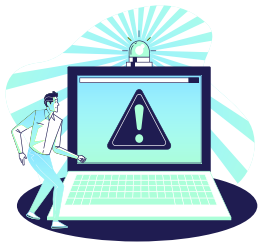
MISSÃO:

- promover o estudo, a discussão e a divulgação das temáticas associadas à *Competitive Intelligence* e à Guerra de Informação
- fomentar o conhecimento nestas áreas para estimular a sua evolução, para fins de desenvolvimento económico e social.

Pós–Graduação: CiberSegurança e Incidentes Cibernéticos

Módulos	H
Gestão de Cibersegurança	42
Gestão do risco, Preparação e Deteção	49
Resposta operacional	56
Governo, liderança e tecnologias emergentes	35





Glossário:

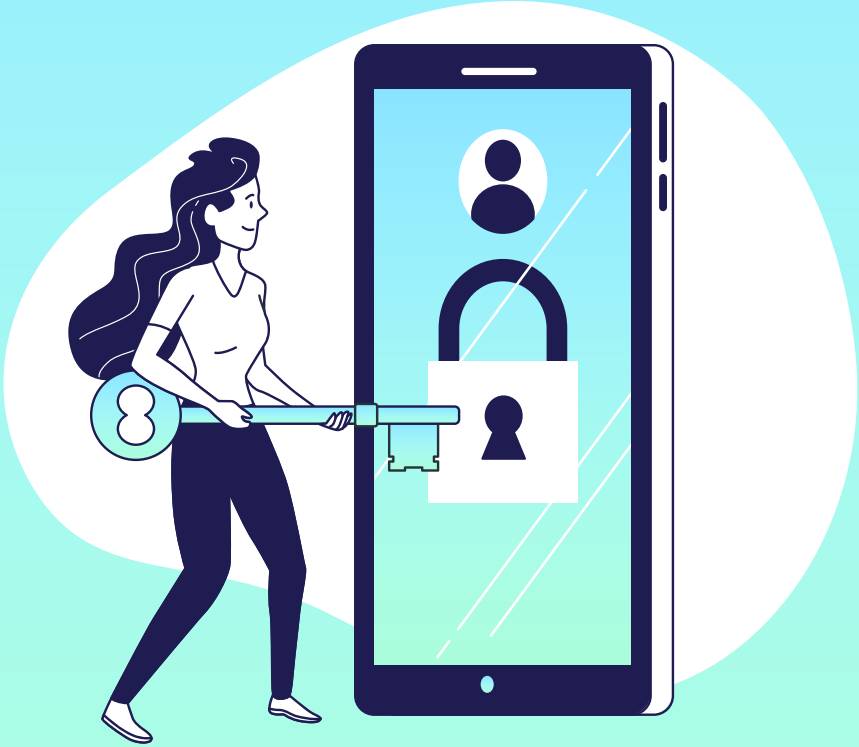
- CERT – Computer Emergency Response Team
- CISO – Chief Information Security Officer
- CNCS – Centro Nacional Cibersegurança
- CSIRT – Computer Security Incident Response Team
- ENISA – European Union Agency for Cybersecurity
- ExNCS – Exercício Nacional de Cibersegurança
- FIRST – Forum of Incident Response and Security Teams
- GNS – Gabinete Nacional de Segurança
- IDS – Intrusion Detection System
- ISAC – Information Sharing and Analysis Centers
- IRT – Incident Response Team
- NIST – National Institute of Standards and Technology
- SIEM – Security Information and Event Management
- SOC – Security Operations Centre

01

PROTEÇÃO

PREVENÇÃO

PROTEÇÃO

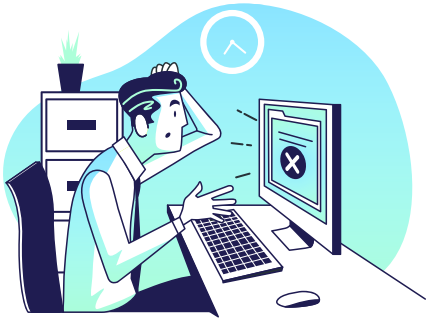


- **CIA Triad**:
  - Confidentiality
  - Integrity
  - Availability

NIST 1977

Segurança da Informação

- **Confidencialidade**: é a garantia de que a informação seja acessível apenas às pessoa autorizadas.
- **Integridade:** é a proteção da informação e dos métodos de processamento quanto a modificações não autorizadas.
- **Disponibilidade**: é a garantia de que as pessoas autorizadas tenham acesso às informações.



PREVENÇÃO

Controlar os acessos a organização, por exemplo, regras na definição das senhas (passwords). Limitar o acesso apenas aos elementos com a revogação das senhas quando necessário.

PROTEÇÃO

As alterações de senhas devem ser criteriosamente geradas e auditadas, Prever acessos internos e externos , remotos, com utilização de dispositivos pessoais. Incluir novos equipamentos configurando-os de forma segura.

AVALIAÇÃO DE SEGURANÇA

Conhecer o Impacto potencial da exposição dos riscos a qual que a organização está sujeita. Avaliar o Risco e as ameaças externas. Descobrir na darkweb informações comprometidas, emails e passwords.

MATURIDADE DA EMPRESA

Identifica na matriz de risco, atribuir um score customizado com base nas categorias selecionadas.

IMPLEMENTAÇÃO DE SOLUÇÕES

Após conhecer o incidente devem ser implementadas medidas para mitigar os danos e reduzir os impactos futuros. Implementar plano de resposta a incidentes definido.

GESTÃO DA SEGURANÇA

Elaboração de uma auditoria detalhada, sendo possível identificar o que aconteceu e tirar lições para o futuro.

02

TIPOS DE ATAQUES

Métodos
Técnicas

ISTEC Instituto Superior de Tecnologias Avançadas do Porto

Classificação de Incidentes

TAXONOMIA

CNCS Centro Nacional de Cibersegurança PORTUGAL

CERT.PT Centro Nacional de Cibersegurança PORTUGAL

Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Compromisso de Conta Privilegiada
	Compromisso de Conta Não Privilegiada
	Compromisso de Aplicação
	Arrombamento
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de Login
	Nova assinatura de ataque

Classe Incidente	Tipo Incidente
Segurança da Informação	Acesso não autorizado
	Modificação não autorizada
	Perda de dados
Fraude	Utilização indevida ou não autorizada de recursos
	Direitos de autor
	Utilização ilegítima de nome de terceiros
	Phishing
Conteúdo Abusivo	SPAM
	Discurso Nocivo
	Exploração sexual de menores, racismo e apologia da violência

Classe Incidente	Tipo Incidente
Vulnerabilidade	Criptografia fraca
	Amplificador DDoS
	Serviços acessíveis potencialmente indesejados
	Revelação de informação
	Sistema vulnerável
Outro	Sem tipo
	Indeterminado

O CERT.PT utiliza para a sua classificação de incidentes a taxonomia da Rede Nacional de CSIRT. Para mais detalhes/informação acerca da Taxonomia em vigor existe um documento disponível no website da RNCSIRT.

Ameaças Acidentais

- Falhas de equipamento
- Erros humanos
- Falhas do Software
- Falhas de alimentação
- Problemas causados pelas forças da natureza

Ameaças Causadas por Pessoas

- Crimes
- Erros dos Utilizadores
- Empregados insatisfeitos
- Vandalismo
- Terrorismo
- Espionagem

White Hat: especialista em informática; auxilia entidades a encontrar vulnerabilidades. São considerados "hackers éticos".

Black Hat (hacker mal-intencionado): utilizam vulnerabilidades para obter dados sigilosos, como dados pessoais, senhas, bancários. São definidos, por alguns autores, como subcategoria dos ***crackers***.

Gray Hat: quando encontram vulnerabilidades, oobservam os dados, e por vezes até os divulga, mas sem cometer crime. Contudo, não informa a entidade sobre a existência da vulnerabilidade.

Script Kiddies: Utilizam ferramentas desenvolvidas por um "***black hat***", sem saber como funcionam. Visam obter publicidade e fama quando conseguem invadir um site importante.

Hacktivistas: agem por motivos ideológicos.

Cracker: pertence ao "lado negro". Responsáveis pela criação dos **cracks**, ferramentas utilizadas na quebra da ativação de um software comercial, para pirataria. São criminosos, que operam em fraudes bancárias, furto de dados, golpes, entre outros.

Phreaker: especialista em redes de comunicação (móvel ou fixa). Visam a utilização do serviço telefónico gratuitamente.

Carder: especialista em fraudes por cartão de crédito. Usam cartões crédito em sites de compras; geram cartões/dados falsos e clonam cartões válidos/verdadeiros.

State Sponsored Hackers (Hackers patrocinados pelo Estado): hackers contratados pelo governo afim de executarem ataques contra outros países, bem como para defender o seu próprio.

Spy Hacker: hackers contratados por empresas para obterem dados sigilosos de empresas concorrentes.

Spammers: enviam e-mails em massa com propagandas de lojas, revistas, produtos em geral, etc.

Vulnerability Searching

- ExploitDB
- NVD
- CVE Mitre

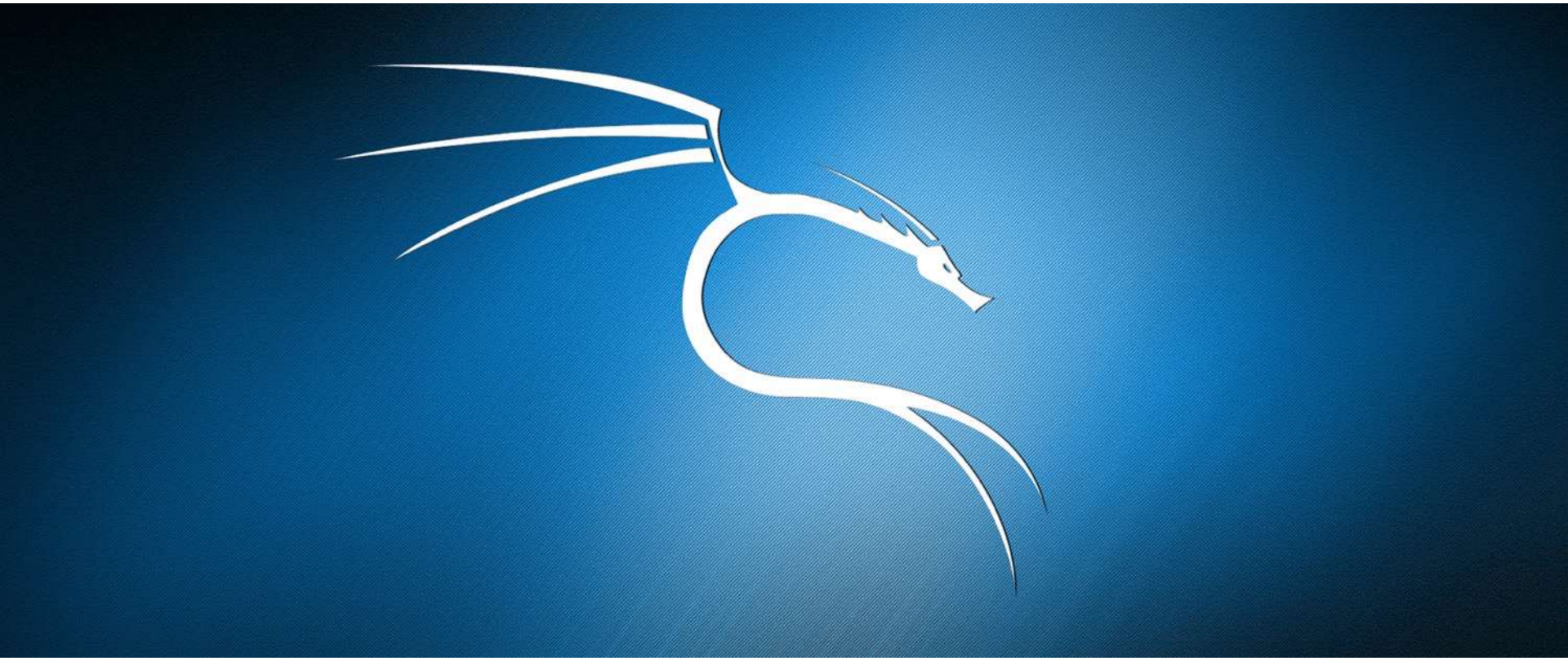
NVD (NIST) contém a listagem dos CVEs (Common Vulnerabilities and Exposures) no formato: CVE-YEAR-IDNUMBER

ExploitDB é especialmente útil para hackers, posi contém "exploits" para download.

It tends to be one of the first stops when you encounter software in a CTF or pentest.

Quem usar CLI no Linux, Kali já trá pré-instalado "searchsploit" para explorar ExploitDB offline, baseado numa database descarregada da internet; assim, já tem tudo pronto a utilizar no seu Kali Linux!

KALI LINUX – Information Security Tools



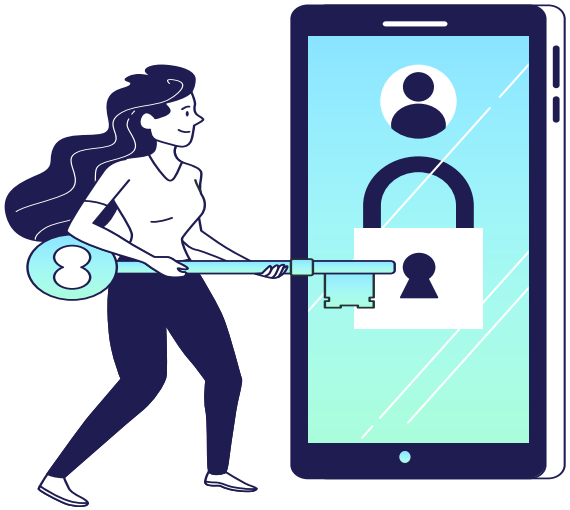
Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Download Documentation

KALI LINUX – Information Security Tools

DNSMAP - scans a domain for common subdomains using a built-in or an external wordlist. The internal wordlist has around 1000 words as ns1, firewall and smtp. Results can be saved in CSV and human-readable format for further processing.

Mainly meant to be used by pentesters during the information gathering/enumeration phase of infrastructure security assessments. During the enumeration stage, the security consultant would typically discover the target company's IP netblocks, domain names, phone numbers, etc.

Subdomain brute-forcing is another technique that should be used in the enumeration stage, as it's especially useful when other domain enumeration techniques such as zone transfers don't work (I rarely see zone transfers being publicly allowed these days by the way).



KALI LINUX – Information Security Tools

DNSMAP - This package provides two possible commands: **dnsmap** and **dnsmap-bulk**.

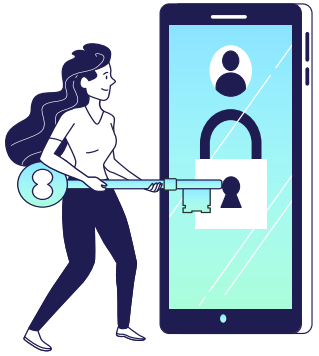
Fun things that can happen:

1. Finding interesting remote access servers (e.g.: https:://extranet.example.com).
2. Finding badly configured and/or unpatched servers (e.g.: test.example.com).
3. Finding new domain names which will allow you to map non-obvious/hard-to-find netblocks of your target organization (registry lookups - aka whois is your friend).
4. Sometimes you find that some bruteforced subdomains resolve to internal IP addresses (RFC 1918). This is great as sometimes they are real up-to-date "A" records which means that it is possible to enumerate internal servers of a target organization from the Internet by only using standard DNS resolving (as opposed to zone transfers for instance).
5. Discover embedded devices configured using Dynamic DNS services (e.g.: IP Cameras). This method is an alternative to finding devices via Google hacking techniques.

This program is useful for pentesters, ethical hackers and forensics experts. It also can be used for security tests.

KALI LINUX – Information Security Tools

DNSENUM - Dnsenum is a multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks. The main purpose of Dnsenum is to gather as much information as possible about a domain.



The program currently performs the following operations:

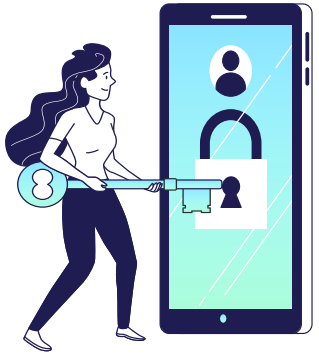
1. Get the host's addresses (A record).
2. Get the namservers (threaded).
3. Get the MX record (threaded).
4. Perform axfr queries on nameservers and get BIND versions(threaded).
5. Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").
6. Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
7. Calculate C class domain network ranges and perform whois queries on them (threaded).
8. Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
9. Write to domain_ips.txt file ip-blocks.

This program is useful for pentesters, ethical hackers and forensics experts. It also can be used for security tests.

KALI LINUX – Penetration Testing

WPSCAN – Permite encontrar vulnerabilidades em websites desenvolvidos com base na framework WordPress.

Exemplo: website feito com Wordpress, da AAAISEP



03

RESPOSTA AO INCIDENTE

Avaliação informática
Consultoria Jurídica
Avaliação de Danos

Envolvimento das várias áreas da Organização

Investigação informática

Serviço especializado pós-incidente, técnicas forenses para realização da gestão dos danos. O que foi roubado? Palavras-passe comprometidas? Pedido de resgate?

Consultoria Jurídica

Tendo em conta o RGPD, se for detetada uma violação dos dados que possam representar risco para terceiros, o prazo é de 72 horas para notificar a CNPD, em Portugal.

Avaliação de Danos Mitigar as perdas financeiras

Instituir o programa de apoio para recuperação da organização conforme existia anterior do incidente.Cuidado acrescido após incidente, na continuidade do negócio e na comunicacao, monitorizando o risco reputacional.

Threat Modelling & Incident Response

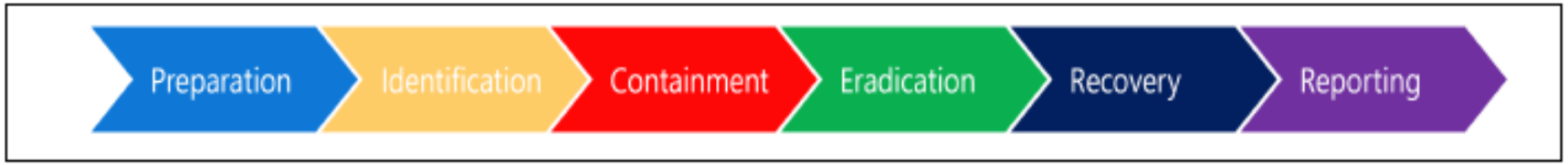
IR: Incident Response
CSIRT: Computer Security Incident Response Team (CSIRT)

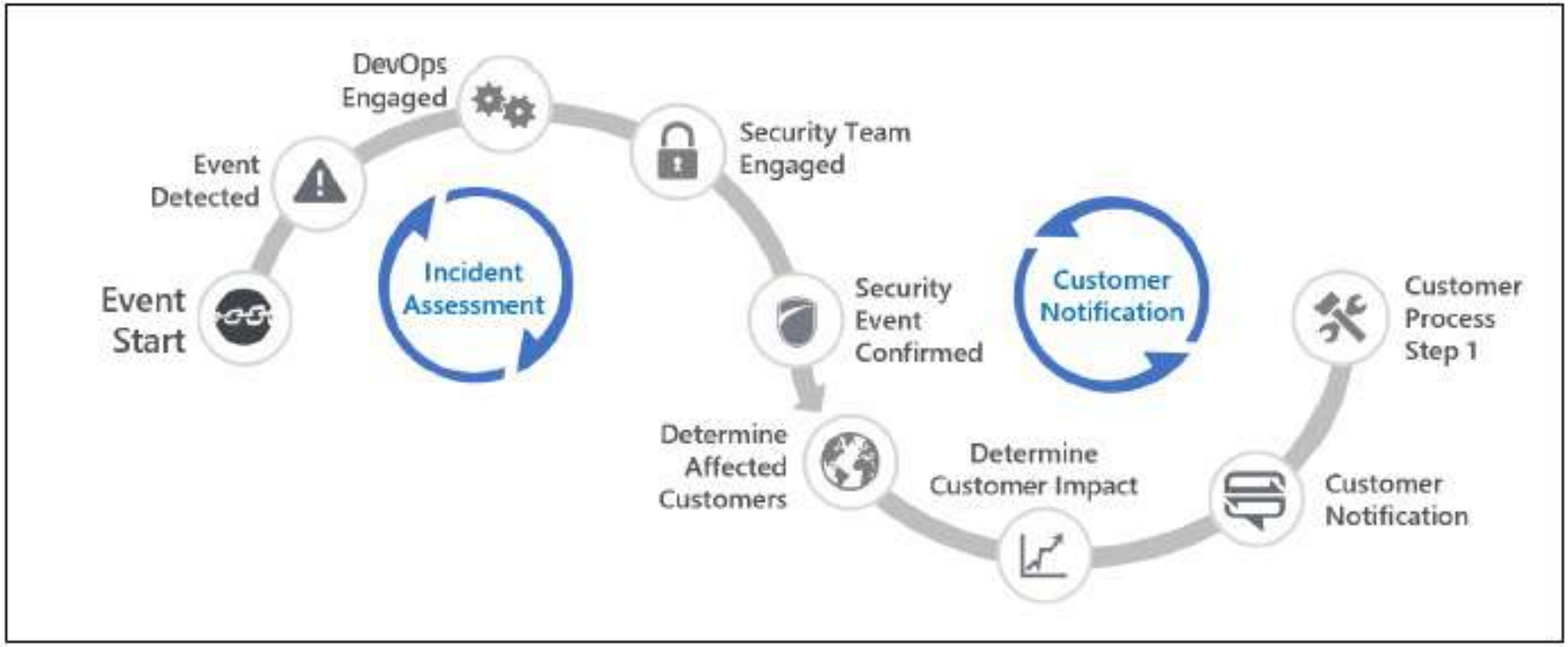
The threat modelling process is very similar to a risk assessment made in workplaces for employees and customers. The principles all return to:

- Preparation
- Identification
- Mitigations
- Review

Components of an incident response plan

Based on the NIST framework, there are six components to an IR plan. These are preparation, identification, containment, eradication, recovery, and reporting:




DevOps Engaged
Event Detected
Event Start
Incident Assessment
Security Team Engaged
Security Event Confirmed
Customer Notification
Customer Process Step 1
Determine Affected Customers
Determine Customer Impact
Customer Notification

04

PLANO DE RECUPERAÇÃO

Interrupção Negócio
Responsabilidades para terceiros
Despesas na resposta ao incidente

INFORMÁTICA

Especialistas em redes informáticas e cibersegurança

ADVOCACIA

Assessoria jurídica Especializada na comunicação, reclamação de terceiros e avaliação de impacto RGPD

PERITOS AVALIADORES DANOS

Mitigar perdas financeiras e orientar ações na recuperação rápida da empresa.

05

RESPONSABILIDADE

Avaliação do Risco Cibernético
Seguros

ANTES

A exposição ao Risco não era objeto de preocupação da administração. A Estratégia de mitigação do Risco era secundária.

DEPOIS

A transferência do Risco é uma realidade, limitando a interrupção do negócio, reduzindo as perdas financeiras.

ANÁLISE

Qual o impacto potencial dos riscos que a organização está exposta? Como está o nível de maturidade de segurança?

TESTE

As soluções tecnológicas introduzidas devem ser testadas e verificadas regularmente, descobrindo as vulnerabilidades desconhecidas.

MELHORIA

Melhorar os procedimentos de segurança informática, realizar simulacros de ataques e testar o nível de preparação para responder.

RGPD

Comissão Europeia

PT português

Pesquisa

Home > ... > Administrações públicas e proteção de dados >

Quais são os principais aspetos do Regulamento Geral sobre a Proteção de Dados (RGPD) de que as administrações públicas devem estar cientes?

Quais são os principais aspetos do Regulamento Geral sobre a Proteção de Dados (RGPD) de que as administrações públicas devem estar cientes?

CONTEÚDO

Resposta

As administrações públicas estão sujeitas às regras do RGPD sempre que efetuam o tratamento de dados pessoais relacionados com um indivíduo. Cabe às administrações públicas nacionais a responsabilidade de prestar apoio às administrações regionais e locais na preparação para a aplicação do RGPD.

A maior parte dos dados pessoais detidos pela administração pública são habitualmente tratados com base numa obrigação jurídica ou na medida do necessário para realizar tarefas por motivos de interesse público ou no exercício de autoridade pública de que está investida.

Aquando do tratamento dos dados pessoais, as administrações públicas devem respeitar os **princípios fundamentais**, nomeadamente:

- tratamento equitativo e lícito;
- limitação da finalidade;
- minimização dos dados e conservação dos dados.

Caso os dados sejam tratados com base no disposto na lei, tais disposições devem já assegurar o respeito destes princípios (p. ex., os tipos de dados, o período de conservação e as medidas de salvaguarda adequadas).

RGPD – Lei 93/2021

proteção das pessoas que denunciam violações do direito

Empresas + 50 empregados têm de:

- implementar a Diretriz (Lei 93/2021)
- Canal de denúncias (digital e físico)
- Responsável pelas denúncias

Autarquias com + 50 funcionários e + 10.000 hab

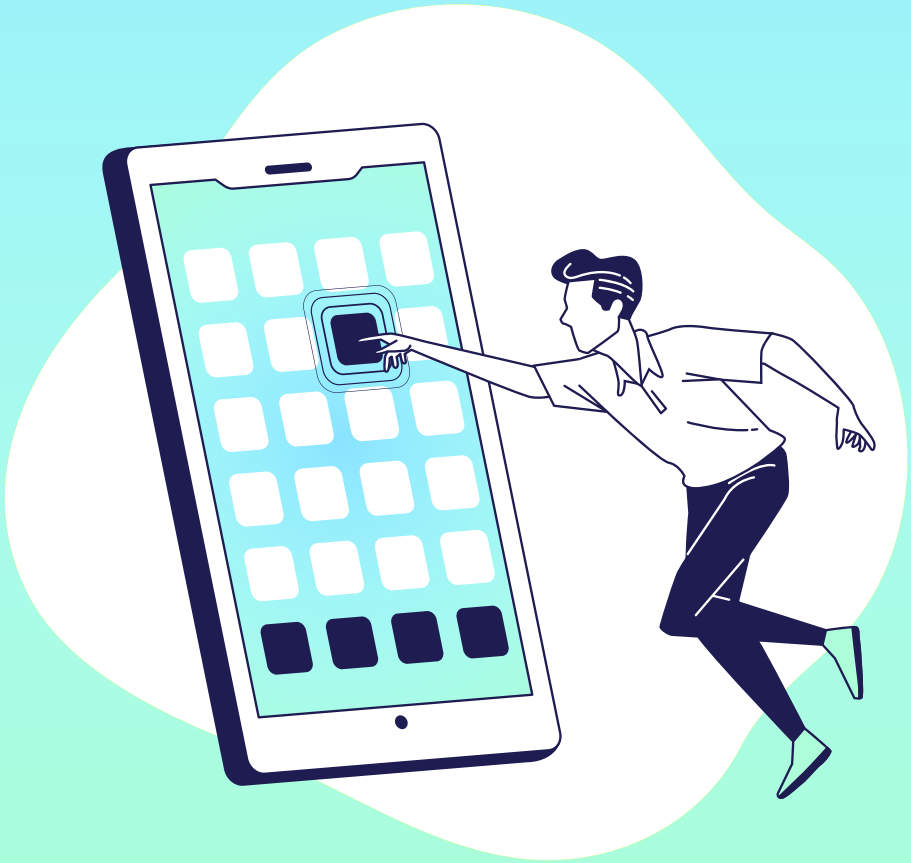
Coimas: até 25.000€ (singulars) e 250.000€ (entidades coletivas)

Período de transição: até 18/6/2022

SUSTENTABILIDADE E CONTINUIDADE DO NEGÓCIO

QUAL É O SEGREDO?

1. Identificação e avaliação dos riscos;
2. Implementação de um plano de redução do impacto do risco na interrupção do negócio;
3. Contratação de uma apólice de seguros capaz de garantir esses riscos;
4. Gestão e regularização do processo de sinistro de forma célere e justa;
5. Elaboração de um plano de ações que permitam recuperar a continuidade do negócio no prazo ideal;



06
PLANO DE PREVENÇÃO

Proteção dos ativos
Roteiro de Capacidades Mínimas

SOLUÇÕES DE CIBERSEGURANÇA

- ❑Testes de intrusão e análise das vulnerabilidades;
- ❑Plataforma centralizada de segurança com mitigação das ameaças;
- ❑Proteção Wi-Fi e Bluetooth;
- ❑Proteção de dados das organizações;
- ❑Validação e análise da segurança de IT;
- ❑Solução para prevenção, deteção e aviso de ciber-ameaças;
- ❑Proteção dos equipamentos e cartões de dados contra as ciber-ameaças;
- ❑Treinar de forma adequada **TODOS** os colaboradores da organização.

Exercício Nacional de Cibersegurança

As atividades referentes ao planeamento e execução do Exercício Nacional Cibersegurança (ExNCS), enquadram-se nas competências orgânicas do CNCS de promover e de assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança e de desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques. O CNCS promove assim o planeamento e a execução do ExNCS ao qual é atribuído um tema de acordo com a relevância atual e necessidades de prevenção. Através destas atividades pretende-se promover o treino e a qualificação de entidades na área da cibersegurança para prevenção e reação a incidentes de cibersegurança, e a formação de uma comunidade de conhecimento e de uma cultura de cibersegurança.

O CNCS participa também no planeamento do exercício Cyber Europe o qual, tal como o ExNCS, simula cenários de incidente em tempo real e serve para avaliar o grau de preparação e de cooperação dos Estados-Membros relativamente à segurança das redes e dos sistemas de informação. O ciclo de exercícios Cyber Europe, é coordenado pela ENISA e serve para testar e participar na elaboração de recomendações sobre a forma como deve evoluir o tratamento de incidentes entre Estados-Membros.









Capture the Flag

A iniciativa "Cyber Security Challenge PT" resulta de uma estreita cooperação entre o Centro Nacional de Cibersegurança, com parceiros do ensino, da Academia e comunidade de Cibersegurança,. Esta iniciativa conta ainda com a parceria do Consórcio Centro Internet Segura.

Trata-se de uma iniciativa que se insere no eixo Educação do programa INCoDe.2030, que visa treinar e formar as camadas mais jovens da população através do estímulo e reforço nos domínios da literacia digital e das competências digitais em todos os ciclos de ensino e de aprendizagem ao longo da vida. Desta forma, a iniciativa pretende identificar jovens talentos nacionais e promover a carreira profissional na área de Cibersegurança.

Anualmente, o "Cyber Security Challenge PT" promove uma competição de "Capture The Flag" (CTF), onde os participantes testam as suas competências nas várias áreas da segurança informática permitindo o desenvolvimento de processos de colaboração e trabalho em rede, conduzindo-os ao crescimento individual através da resolução de desafios complexos.

NO MORE RANSOM!

O website "No More Ransom" é uma iniciativa da Unidade de Crime de Alta Tecnologia da Polícia Holandesa, do European Cybercrime Centre (EC3) da Europol, Kaspersky e McAfee com o objetivo de ajudar as vítimas de ransomware a recuperar os seus ficheiros cifrados sem terem que pagar a criminosos.

Uma vez que é muito mais fácil evitar a ameaça do que lutar contra ela assim que um sistema é infetado, o projeto também visa educar os utilizadores sobre como é que o ransomware funciona e quais as medidas que podem ser tomadas para uma prevenção efetiva. Quantos mais parceiros se juntarem ao projecto, melhores resultados poderão ser obtidos.
Esta iniciativa é aberta a parceiros públicos e privados.

O Centro Nacional de Cibersegurança também é parceiro do projeto "No More Ransom".

Critical Infrastructures and Services

A smart grid is an upgraded electricity network depending on two-way digital communications between supplier and consumer that in turn give support to intelligent metering and monitoring systems. Smart grids give clear advantages and benefits to the whole society, but the dependency on computer networks and the Internet into future grids makes our society more vulnerable to malicious attacks with potentially devastating results.

ENISA has issued reports of the following areas of smart grid security:

- Smart Grid Security Certification in Europe
- Smart Grid Security: Recommendations for Europe and Member States
- Appropriate security measures for smart grids
- Communication network interdependencies in smart grids

Roteiro de criação de capacidades mínimas (i)

1.Preparação

- Ligação CNCS
- Identif. quadro de Ameaças

2.Arquitetura de Segurança

- Arquitetura de Segurança

3.Implementação

- Deteção e prevenção de ameaças
- Definição de capacidades
- Mecanismos de audioria
- Mecanismos de alerta

4.Procedimentos e políticas

5.Equipas

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 1 - PREPARAÇÃO

A 1.1 - Formalização de Protocolo de Colaboração e Adenda

A 1.2 - Identificação de RESPONSÁVEL DE SEGURANÇA

A 1.3 – Identificação de funções ou atividades críticas

A 1.4 - Estabelecimento de canais de comunicação

A 1.5 - Registo de endereços de IP no LIR (Local Internet Registry)

A 1.6 - Estabelecimento de metodologia de Análise de Risco

A 1.7 – Cadeia de responsabilidade: preparação

A 1.8 – Definição de política de segurança de informação

A 1.9 – Procedimentos de notificação de incidentes

Roteiro de criação de capacidades mínimas (ii)

FASE 2 – ARQUITETURA DE SEGURANÇA

A 2.1 – Desenho e implementação da segurança perimétrica
A 2.2 – Implementação de sistema de recolha e armazenamento do fluxo de tráfego
A 2.3 – Comunicação com o CNCS
A 2.4 – Inventariação de ativos / produção de um mapa de rede
A 2.5 – Recolha centralizada de registos (logs)
A 2.6 – Criação de instrumentos de correção ou mitigação de incidentes
A 2.7 – Estabelecimento de conformidade com a legislação aplicável
A 2.8 – Estabelecimento de conformidade com normas aplicáveis à área de atividade
A 2.9 – Criação de política de uso aceitável
A 2.10 – Manutenção de infraestruturas de cópias de segurança e repo (Backup/Restore)
A 2.11 – Mapa de competências e planos de formação
A 2.12 – Treino e sensibilização interna: geral
A 2.13 – Treino e sensibilização interna: gestão

Roteiro de criação de capacidades mínimas (ii)

FASE 3 – IMPLEMENTAÇÃO

A 3.1 – Definição de procedimentos de operação

A 3.2 – Instalação e configuração de sensores em dispositivos

A 3.3 – Auditoria de segurança e Bases de Dados

A 3.4 – Instalação e configuração de controlo de acessos web – (e.g. serviços proxy)

A 3.5 – Proteção e gestão de equipamentos

A 3.6 – Instalação e configuração de mecanismos de monitorização

A 3.7 – Hardening das configurações

A 3.8 – Instalação e configuração de um Security Information and Event Management (SIEM)

A 3.9 – Definição de planos de continuidade de negócio

A 3.10 – Aquisição de competências técnicas

Roteiro de criação de capacidades mínimas (ii)

FASE 4 – PROCEDIMENTOS E POLÍTICAS

A 4.1 – Cadeia de responsabilidades: formalização

A 4.2 – Definição do Sistema Interno de Normas e Políticas (SINP)

A 4.3 – Análise de risco - reavaliação

A 4.4 – Simulacro

A 4.5 – Definição de procedimentos de reação a incidentes

A 4.6 – Treino e sensibilização interna: SINP

A 4.7 – Testes de aceitação de serviços

A 4.8 – Mecanismos de engodo (honeypots)

A 4.9 – Gestão de mudanças e atualizações

Roteiro de criação de capacidades mínimas (ii)

FASE 5 – EQUIPAS

A 5.1 – Nomear um CISO (*Chief Information Security Officer*)

A 5.2 – Estabelecer um serviço de gestão de vulnerabilidades

A 5.3 – Estabelecer e implementar um plano de auditorias

A 5.4 – Definir a missão, a comunidade servida e o portfólio de serviços do CSIRT

A 5.5 – Elaborar e fazer aprovar o plano e o orçamento para o CSIRT

A 5.6 – Montar e anunciar o CSIRT

A 5.7 – Estabelecer um sistema de gestão de Crise

A 5.8 – Afiliação nas comunidades nacionais e internacionais de CSIRT

A 5.9 – Participação num exercício nacional de cibersegurança

CSIRT – *Computer Security Incident Response Team*

Roteiro de criação de capacidades mínimas (ii)

FASE 5 – EQUIPAS

A 5.1 - CISO (*Chief Information Security Officer*) terá a seu cargo a gestão da segurança de informação, como responsável máximo. A governação da segurança de informação numa organização com elevado grau de complexidade ou dimensão necessita deste destaque e autonomia como contraponto a outros legítimos interesses relacionados com a gestão interna da organização.

O CISO deve ser o topo da hierarquia no que toca à governação de segurança, e o elemento da direção a quem reporta o SOC ou CSIRT.

CSIRT – Computer Security Incident Response Team

SOC – Security Operations Centre

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase I

- Coopere com o CNCS numa base sistemática e tenha definido um ponto de contacto
- Tenha a noção dos principais ativos da organização
- Disponha de bases normativas internas para a proteção destes ativos críticos e da segurança de informação interna como um todo.

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase II

- Intensifique o nível de cooperação com o CNCS com o estabelecimento de comunicações a nível operacional
- Proteja o perímetro da sua rede
- Disponha de informação de registo e fluxos de tráfego que permitem uma deteção atempada de ameaças, bem como o diagnóstico a posteriori do comportamento dos sistemas internos perante um evento de segurança
- Faça uma apropriada gestão e inventariação de ativos de informação internos, complementada com esquemas ou mapas da Rede
- Previna permanente os Riscos de inconformidade com a Lei e normativos ou certificações aplicáveis
- Disponha de resiliência ao nível da disponibilidade e integridade de informação, através da criação e manutenção de procedimento de backup e restore
- Acautele a formação dos recursos humanos internos de acordo com um mapa de competências

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase III

- Assegure a integridade e nível de segurança de sistemas aplicacionais internos
- Gira centralmente os equipamentos que suportam ativos de informação de
- forma eficiente
- Garanta a bom funcionamento dos equipamentos de suporte à infraestrutura de Rede
- Controle e centralize de forma eficaz a informação de eventos de segurança provenientes dos vários dispositivos e equipamentos de suporte à infraestrutura TIC num sistema SIEM
- Tenha equipas internas encarregadas da segurança de informação com formação nos domínios especializados da cibersegurança

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase IV

- Gira eficientemente os processos operacionais de segurança interna através da constituição formal de procedimentos
- Integre as políticas e normativos definidos em fases anteriores apropriadamente dentro de um quadro de gestão
- Garanta a manutenção da aplicação da metodologia de gestão de risco
- previamente definida
- Gira apropriadamente processos de mudança, incluindo a aplicação de patches e atualizações de segurança regulares
- Abranja a segurança de dispositivos móveis no quadro das medidas tecnológicas e processuais
- Condicione a entrada em produção de sistemas mediante a aplicação de testes de segurança e consequente aceitação por parte de uma equipa especializada
- Disponha de colaboradores sensibilizados nas áreas gerais de cibersegurança que tocam o desempenho das respetivas funções profissionais
- Disponha de hierarquias sensibilizadas para a importância da manutenção de um elevado nível de preparação e defesa ao nível da cibersegurança

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase V

- Disponha de um responsável máximo pela segurança de informação (CISO)
- Assegure a eficaz gestão de incidentes e vulnerabilidades, através da criação de uma equipa especializada (CSIRT)
- Conte com um sistema de gestão de crise nos processos internos

Roteiro de criação de capacidades mínimas (ii)

RESUMO POR FASES (sumário de capacidades)

Fase V

- Disponha de um responsável máximo pela segurança de informação (CISO)
- Assegure a eficaz gestão de incidentes e vulnerabilidades, através da criação de uma equipa especializada (CSIRT)
- Conte com um sistema de gestão de crise nos processos internos

Glossário:

- CERT – Computer Emergency Response Team
- CISO – Chief Information Security Officer
- CNCS – Centro Nacional Cibersegurança
- CSIRT – Computer Security Incident Response Team
- ENISA – European Union Agency for Cybersecurity
- ExNCS – Exercício Nacional de Cibersegurança
- FIRST – Forum of Incident Response and Security Teams
- GNS – Gabinete Nacional de Segurança
- IDS – Intrusion Detection System
- ISAC – Information Sharing and Analysis Centers
- IRT – Incident Response Team
- NIST – National Institute of Standards and Technology
- SIEM – Security Information and Event Management
- SOC – Security Operations Centre

Bibliografia / Artigos e relatórios técnicos / Sítios da Inte

Livros

- Thakur, K., & Pathan, A.-S. K. (2020). ***Cybersecurity fundamentals : a real-world perspective***. Taylor & Francis.
- Daswani, N., & Elbayadi, M. (2021). **Big Breaches: Cybersecurity Lessons for Everyone**. In *Big Breaches* (Springer S). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6655-7_1
- Ozkaya, E. (2021). ***Incident Response in the Age of Cloud***. Packt Publishing.

Artigos e relatórios técnicos

- CNCS – Centro Nacional de Cibersegurança (2019). **Roteiro para Capacidades Mínimas de Cibersegurança.** https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf
- DGEEC, (2021). ***A Segurança das TIC (Cibersegurança) na administração pública central, regional e câmaras municipais*** - *IUTICAP e IUTICCM 2020*.
- ISO & IEC (2005). *ISO/IEC 17799:2005(E) Information technology — Security techniques —* ***Code of practice for information security management***.
- Lande, D., & Shnurko-Tabakova, E. (2019). **OSINT as a part of cyber defense system.** *Theoretical and Applied Cybersecurity*, *1*(1), 103–108. https://doi.org/10.20535/tacs.2664-29132019.1.169091
- Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001
- Marta Barceló, Board member, I., & Pete Herzog, Director, O. (n.d.). ***OSSTMM 3 – The Open Source Security Testing Methodology Manual***.

Sítios da Internet:

- https://www.kali.org/docs/tools/kali-tools/
- https://tryhackme.com/
- https://www.cncs.gov.pt/

Webinar – CIBERSEGURANÇA
ISTEC Porto / CITECA

Objetivos a atingir:

1. Compreender em que consiste a Cibersegurança ✓
2. Saber quais são os riscos e as ameaças ✓
3. Conhecer os tipos de ataques mais frequentes ✓
4. Demonstração de algumas das ferramentas para testes de intrusão e deteção de vulnerabilidades (Kali Linux) ✓
5. Enquadramento da responsabilidade legal pela salvaguarda e proteção dos dados (RGPD) ✓
6. Ficar a conhecer planos de resposta ao incidente, recuperação de dados e retoma da normalidade ✓

OBRIGADO PELA ATENÇÃO!

João Emílio Almeida, Eng Ph.D
ISTEC Porto / CITECA