

CONFERÊNCIA

CIBERSEGURANÇA: preparar o presente para os desafios do futuro



MÊS EUROPEU
DA CIBERSEGURANÇA
OUTUBRO

MÊS EUROPEU DA CIBERSEGURANÇA

CIBERSEGURANÇA NAS ORGANIZAÇÕES

Do risco à resiliência

Diana Alves

Analista de Cibersegurança · CERT.PT | CNCS



CONTEXTO

O que é o CERT.PT

Equipa de resposta a incidentes

O CERT.PT é a Equipa de Resposta a Incidentes de Cibersegurança do Centro Nacional de Cibersegurança.

COMUNIDADES SERVIDAS

Entidades públicas relevantes

Entidades essenciais e importantes

Restante ciberespaço de interesse nacional



Coordenação de resposta

Apoio na gestão de incidentes, articulando os vários intervenientes.



Alertas

Avisos e recomendações sobre ameaças e campanhas em curso.



Vulnerabilidades

Identificação e notificação de sistemas expostos ou vulneráveis.



Suporte on-site

Apoio presencial em incidentes de maior impacto.

ÍNDICE

- 01 Os riscos que hoje vemos nas organizações
- 02 Boas práticas e como reportar
- 03 Tendências para o futuro próximo



OS RISCOS DE HOJE

Os incidentes não param de crescer



Fonte: CERT.PT / Observatório de Cibersegurança do CNCS · incidentes notificados, excluindo fontes automatizadas

61798

incidentes registados em 2025

3864

incidentes manuais

+40%

face a 2024 (2 758)

≈ 9×

mais do que em 2016 (413)

OS RISCOS DE HOJE

As 5 ameaças mais relevantes

01

Phishing e smishing

Mensagens que imitam entidades legítimas para roubar credenciais.

02

Engenharia social e burlas

Falsos fornecedores, falsos diretores, falsos familiares.

03

Ransomware

Cifra e rouba dados para extorquir a organização.

04

Exploração de falhas

Vulnerabilidades por corrigir em sistemas expostos à Internet.

05

Negação de serviço distribuída (DDoS)

Indisponibilidade de serviços online.

Principais agentes de ameaça:

Cibercriminosos

Hacktivistas

Atores estatais

Fonte: Relatório do Observatório de Cibersegurança do CNCS, setembro de 2025 (dados de 2024)

Comprometimento de conta

Como acontece

Palavras-passe fracas ou reutilizadas

A mesma usada noutro serviço.

Fugas de dados de terceiros

Credenciais expostas noutros sites.

Credential stuffing

Bots testam combinações roubadas.

Infostealers

Malware que rouba palavras-passe e sessões.

Boas práticas

- Palavras-passe longas e únicas
- Gestor de palavras-passe aprovado
- MFA em todas as contas
- Separar contas pessoais e de trabalho
- Verificar em haveibeenpwned.com
- Reportar um acesso suspeito

Phishing e smishing

Como funciona

Emails ou mensagens que imitam entidades legítimas para roubar credenciais ou dados.

SINAIS DE ALERTA

- Urgência ou ameaça
- Link encurtado
- Pede credenciais
- Domínio parecido

Boas práticas

- Aceder sempre pelo site ou app oficial
- Verificar o domínio antes de clicar
- Nunca partilhar códigos de acesso
- Filtros anti-phishing no email
- Simulações de phishing na equipa
- Canal simples para reportar

Mais imitados em 2025: Energia · Banca · Operadores de Telecomunicações · Saúde

Ransomware

O que é

Malware que cifra os sistemas e exige um resgate. Hoje, quase sempre, os dados são roubados antes (dupla extorsão).

IMPACTO

- Operação parada
- Custos elevados
- Dados publicados
- Danos reputacionais

Boas práticas

- Cópias de segurança
- MFA e atualizações nos acessos remotos
- Menos contas com privilégios
- Formação contra phishing

Não pagar o resgate: não garante a recuperação. Ferramentas gratuitas: nomoreransom.org

Exploração de vulnerabilidades

Porque acontece

Falhas conhecidas, muitas vezes já com correção disponível, ficam por aplicar em sistemas expostos à Internet.

ALVOS FREQUENTES

- VPN e acesso remoto
- Firewalls e routers
- Servidores de email
- Sites desatualizados

Boas práticas

- Inventário do que está exposto à Internet
- Corrigir primeiro o crítico e exposto
- Acompanhar os alertas do CERT.PT
- Retirar equipamentos sem suporte
- MFA nos acessos remotos
- Testes de vulnerabilidades regulares

Fim de suporte é fim das correções: um equipamento sem atualizações é uma porta aberta.

Negação de serviço distribuída (DDoS)

Como funciona

Inundar um site ou serviço com tráfego até ficar indisponível — muitas vezes por motivação hacktivista.

IMPACTO

- Site e loja em baixo
- Clientes sem serviço
- Danos reputacionais
- Desvio de atenção

Boas práticas

- Proteção anti-DDoS com o ISP ou CDN
- Saber quem contactar no fornecedor
- Monitorizar o tráfego e ter alertas
- Separar serviços críticos do site
- Plano de comunicação a clientes
- Reportar ao CERT.PT

CEO Fraud

Como funciona

Alguém finge ser a administração, um fornecedor ou colaborador e pede um pagamento urgente — muitas vezes para um IBAN “novo”.

SINAIS DE ALERTA

- Urgência e sigilo
- IBAN alterado por email
- Remetente parecido
- Fora do circuito habitual

Como evitar o pagamento

- Confirmar IBAN novo por telefone conhecido
- Nunca usar os contactos do email
- Dupla autorização em pagamentos
- Pedir comprovativo de titularidade
- Se já pagou: ligar logo ao banco



QUANDO ACONTECE

A quem reportar?

1

CERT.PT

cert@cert.pt e MyCiber — apoio técnico e alerta a outras entidades.

2

Polícia Judiciária

Sempre que haja crime: fraude, extorsão ou intrusão.

3

CNPD

Sempre que houver exfiltração ou exposição de dados pessoais.

4

Banco

De imediato, em fraudes de pagamento.



O QUE AÍ VEM

Tendências para o futuro próximo

01 Cloud e terceiros

Mais ataques a infraestruturas cloud e à cadeia de fornecimento.

02 Superfície de ataque

Mais sistemas expostos, mais vulnerabilidades exploradas.

03 Infostealers

Roubo e comércio online de credenciais.

04 Criptomoedas

Um uso crescente que potencia o cibercrime.

05 IA generativa

Usada para preparar e escalar ciberataques.

06 Desinformação

Mudanças nas políticas das plataformas podem potenciá-la.

Fonte: Relatório do Observatório de Cibersegurança do CNCS, setembro de 2025

OBRIGADO/A

Pela participação

Diana Alves · CERT.PT | Centro Nacional de Cibersegurança

14 OUTUBRO · ISCAP, PORTO



MÊS EUROPEU
DA CIBERSEGURANÇA
OUTUBRO