



**Departamento de Engenharia Informática e de  
Sistemas**

**Instituto Superior de Engenharia de  
Coimbra**

**Instituto Politécnico de Coimbra**

**Licenciatura em Engenharia Informática**

**Curso Diurno**

**Ramo de Sistemas de Informação**

**Unidade Curricular de Ética e Deontologia**

**Ano Letivo de 2023/2024**

**PALESTRA N.º 8**

**Ciber Segurança e Proteção de Infraestruturas Críticas**

**Eng.º Paulo Moniz**

**Realizada em 24 de abril de 2024**

**DESAFIOS E ESTRATÉGIAS EM CIBER SEGURANÇA**



**Dinis Meireles de Sousa Falcão**

**2020130403**

**Coimbra, 01 de maio de 2024**

**DINIS MEIRELES DE SOUSA FALCÃO**

**DESAFIOS E ESTRATÉGIAS EM CIBER SEGURANÇA**

Ética e Deontologia

**Coimbra, 01 de maio de 2024**

## Índice

RESUMO .....	iv
1. INTRODUÇÃO .....	5
2. DESCRIÇÃO DO TEMA ABORDADO NA PALESTRA .....	7
2.1. Desafios e Estratégias em Ciber Segurança .....	7
2.2. Contextualização da EDP .....	7
2.3. Ciber Riscos e Vulnerabilidades .....	8
2.4. Tipos e Sofisticação dos CiberAtaques .....	9
3. ANÁLISE CRÍTICA.....	11
3.1. Ênfase na Complexidade Operacional.....	11
3.2. Abordagem Proativa versus Reativa .....	11
3.3. Conclusão da Análise Crítica .....	11
4. CONSIDERAÇÕES FINAIS .....	A
REFERÊNCIAS .....	B
ANEXOS .....	B

## RESUMO

Este relatório aborda a palestra proferida pelo Eng.º Paulo Moniz sobre Ciber Segurança e Proteção de Infraestruturas Críticas, com foco na experiência da EDP. A palestra enfatizou a importância de compreender e mitigar os riscos cibernéticos, incluindo vulnerabilidades decorrentes de procedimentos, configurações e dependência de prestadores de serviços externos. A transformação digital introduziu novos desafios, como a necessidade de proteger dados na nuvem e garantir a segurança de uma arquitetura de TI complexa. Os ciberataques representam uma ameaça séria, com atacantes cada vez mais sofisticados, incluindo APTs, ransomware e phishing. Proteger recursos críticos, como dados pessoais e infraestruturas, torna-se essencial para a continuidade dos negócios e a segurança da sociedade.

Palavras-chave: Ciber Risco, Ciber Segurança, Transformação Digital, Ciber Poder, Vulnerabilidades

## 1. INTRODUÇÃO

Esta apresentação destaca os principais pontos abordados na palestra proferida pelo Eng.º Paulo Moniz sobre Ciber Segurança e Proteção de Infraestruturas Críticas. O tema central da palestra é a crescente importância da cibersegurança num ambiente empresarial cada vez mais digitalizado e interconectado.

O Relatório segue uma sequência lógica, começando com uma contextualização da EDP, uma empresa multinacional com presença em 14 países e uma ampla cadeia de valor na indústria de energia. Em seguida, são discutidos os desafios enfrentados pela empresa em termos de Ciber Riscos e Vulnerabilidades, destacando a complexidade das operações e a dependência de prestadores de serviços externos.

O objetivo do Relatório é oferecer uma visão abrangente dos desafios de cibersegurança enfrentados atualmente e apresentar estratégias para mitigar esses riscos.

As partes que compõem o Relatório incluem uma introdução ao tema, uma caracterização da EDP e sua cadeia de valor, uma análise dos Ciber Riscos e vulnerabilidades, uma discussão sobre os tipos e sofisticação dos ciberataques, e uma visão sobre a proteção dos recursos da empresa. Cada parte é elaborada para oferecer uma compreensão clara dos desafios e estratégias em Ciber Segurança.



## 2. DESCRIÇÃO DO TEMA ABORDADO NA PALESTRA

### 2.1. Desafios e Estratégias em Ciber Segurança

A palestra conduzida pelo Eng.º Paulo Moniz centrou-se nos desafios prementes que a EDP enfrenta em termos de segurança cibernética, destacando a importância de estratégias eficazes para proteger suas infraestruturas críticas. A escolha deste tema foi motivada pela crescente interconexão dos sistemas de informação e pela vulnerabilidade das empresas do setor energético a ataques cibernéticos, que podem ter impactos devastadores na prestação de serviços e na segurança dos clientes.

Durante a palestra, o palestrante abordou vários fundamentos teóricos relacionados à cibersegurança, incluindo conceitos de ciber-risco, vulnerabilidades sistêmicas e a evolução das táticas empregadas pelos atacantes cibernéticos. Ele destacou a importância de uma abordagem holística para mitigar esses riscos, envolvendo não apenas medidas técnicas, mas também conscientização dos funcionários e parcerias estratégicas com especialistas em segurança cibernética.

Durante a apresentação, o palestrante seguiu várias linhas de pensamento para abordar os desafios e estratégias em cibersegurança na EDP:

- Identificação de Vulnerabilidades Críticas;
- Resposta Rápida a Incidentes de Segurança;
- Investimento em Tecnologia de Ponta;
- Conscientização dos Funcionários;
- Entre outras.

### 2.2. Contextualização da EDP





A EDP (Energias de Portugal) é uma **empresa multinacional de energia com sede em Portugal**, que opera em diversos países ao redor do mundo. Fundada em 1976, a EDP tornou-se uma das principais empresas do setor energético, fornecendo eletricidade e gás natural para milhões de clientes em todo o mundo. **Com cerca de 12.000 funcionários, a EDP possui uma vasta presença global, atuando em 14 países, incluindo Portugal, Espanha, Estados Unidos e Brasil.** O seu alcance geográfico abrange tanto mercados desenvolvidos quanto emergentes, refletindo assim a sua posição como uma das líderes no setor de energia. (EDP, 2024)

A empresa opera em toda a **cadeia de valor da energia, desde a criação e distribuição até à comercialização**. Por meio das suas subsidiárias e participações, a EDP está envolvida na produção de energia a partir de fontes convencionais, como **termoelétricas e hidroelétricas**, bem como em iniciativas de **energias renováveis**, como a energia eólica e solar.

Além disso, a EDP desempenha um **papel crucial no fornecimento de infraestruturas críticas, como redes elétricas e sistemas de distribuição, que são essenciais para garantir o fornecimento confiável de energia para as empresas e os consumidores em todo o mundo.** A sua posição como uma das maiores empresas de energia na Europa e na América torna-a num alvo potencial para ameaças cibernéticas. Diante deste cenário, a **segurança cibernética torna-se uma preocupação fundamental para a EDP, pois qualquer interrupção nas suas operações pode ter impactos significativos não apenas para a empresa, mas também para a sociedade em geral.** Nesse contexto, compreender os desafios e desenvolver estratégias eficazes de cibersegurança torna-se essencial para garantir a continuidade dos negócios e proteger os interesses dos seus clientes e partes interessadas.

### 2.3. Ciber Riscos e Vulnerabilidades

A EDP enfrenta diversos desafios em termos de **Ciber Riscos e vulnerabilidades**, especialmente devido à natureza complexa das suas operações e à sua dependência de prestadores de serviços externos. Esses desafios podem ser divididos em várias áreas-chave:

-  **Complexidade das Operações:** Como uma empresa multinacional de energia, a EDP opera em diversos países e está envolvida em todas as etapas da cadeia de valor da energia, desde a criação até a distribuição e comercialização. Essa ampla gama de operações cria uma complexidade significativa em termos de infraestrutura de TI e sistemas de informação, tornando-a mais vulnerável a ataques cibernéticos;
-  **Dependência de Prestadores de Serviços Externos:** A EDP depende de uma rede complexa de prestadores de serviços externos, incluindo fornecedores de tecnologia, contratados para diversas funções, como manutenção de sistemas, desenvolvimento de software e serviços de terceirização. Essa dependência aumenta o risco de segurança cibernética, uma vez que **terceiros podem não ter os mesmos padrões rigorosos de segurança que a própria empresa.**
-  **Ampla Superfície de Ataque:** Com uma grande variedade de sistemas e aplicações em operação, a EDP possui uma ampla superfície de ataque que pode ser explorada por hackers e ciber criminosos. Desde sistemas de controle de infraestrutura crítica até redes corporativas e aplicações de negócios, cada componente representa uma potencial vulnerabilidade que pode ser explorada.
-  **Vulnerabilidades em Sistemas Legados:** Como muitas empresas estabelecidas, a EDP pode ter sistemas legados que foram desenvolvidos sem as mesmas preocupações de segurança que os sistemas modernos. Esses sistemas podem conter vulnerabilidades conhecidas ou não corrigidas, tornando-os alvos potenciais para ataques cibernéticos.



## 2.4. Tipos e Sofisticação dos CiberAtaques

Os tipos e a sofisticação dos ciberataques estão em **constante evolução**, representando um desafio significativo para empresas como a EDP. Ao discutir esses aspetos, é importante considerar uma ampla gama de táticas utilizadas pelos ciber criminosos, desde métodos simples até estratégias altamente sofisticadas. Aqui estão alguns dos tipos e tendências de ciberataques relevantes: (Wikipédia, s.d.)

- 🚩 **Ransomware:** Os ataques de ransomware envolvem o uso de malware para criptografar os dados de uma organização e exigir um resgate em troca da chave de descriptografia. Esses ataques podem paralisar as operações da empresa e causar danos financeiros significativos.
- 🚩 **Phishing:** O phishing é uma técnica de engenharia social que visa enganar os utilizadores para que divulguem informações confidenciais, como senhas ou informações de cartão de crédito. Os ataques de phishing podem ser direcionados a funcionários da empresa ou clientes, visando obter acesso não autorizado a sistemas ou roubar dados pessoais.
- 🚩 **Ataques de Negação de Serviço (DoS):** Os ataques de DoS visam sobrecarregar os sistemas de uma empresa, tornando-os inacessíveis para utilizadores legítimos. Esses ataques podem ser realizados por meio do envio de tráfego malicioso em grande escala ou explorando vulnerabilidades em sistemas específicos.
- 🚩 **Ataques de Engenharia Social:** Este tipo de ataque envolve a manipulação psicológica dos indivíduos para obter acesso não autorizado a sistemas ou informações confidenciais. Os ciber criminosos podem passar-se por funcionários legítimos da empresa ou enviar emails fraudulentos para persuadir os utilizadores a tomar ações prejudiciais.
- 🚩 **Ataques Avançados e Persistentes (APT's):** As APT's são ataques altamente direcionados e sofisticados, geralmente patrocinados por estados-nação ou grupos criminosos organizados. Esses ataques podem envolver múltiplas fases e técnicas de evasão para contornar as defesas de segurança tradicionais e obter acesso prolongado aos sistemas da empresa.
- 🚩 **Exploração de Vulnerabilidades de Software:** Os ciber criminosos frequentemente exploram vulnerabilidades conhecidas em software e sistemas desatualizados para ganhar acesso não autorizado a redes corporativas. Isso pode envolver o uso de exploits publicamente divulgados ou o desenvolvimento de malware personalizado para explorar essas vulnerabilidades.



### 3. ANÁLISE CRÍTICA

#### 3.1. Ênfase na Complexidade Operacional

A palestra destacou adequadamente a complexidade das operações da EDP, especialmente sua dependência de prestadores de serviços externos e a ampla superfície de ataque resultante. No entanto, uma análise mais profunda das medidas específicas tomadas pela EDP para mitigar esses riscos teria sido valiosa.

#### 3.2. Abordagem Proativa versus Reativa

Embora a palestra tenha ressaltado a importância da cibersegurança e a necessidade de compreender e mitigar os riscos cibernéticos, uma análise mais aprofundada sobre a abordagem da EDP para cibersegurança teria sido útil. Questões como a integração de políticas de segurança cibernética desde o início do desenvolvimento de novos sistemas e a implementação de programas contínuos de treinamento e conscientização dos funcionários poderiam ter sido exploradas para avaliar a eficácia da empresa na adoção de uma abordagem proativa em vez de reativa à segurança cibernética.

#### 3.3. Conclusão da Análise Crítica

No entanto, a palestra proferida pelo Eng.º Paulo Moniz sobre cibersegurança e proteção de infraestruturas críticas ofereceu uma visão abrangente dos desafios enfrentados pela EDP nesse campo, além de discutir um tema com bastante importância hoje em dia.



#### 4. CONSIDERAÇÕES FINAIS

A palestra sobre cibersegurança e proteção de infraestruturas críticas ministrada pelo Eng.º Paulo Moniz ofereceu uma visão abrangente dos desafios enfrentados pela EDP nesse campo em constante evolução. Ao longo da análise do tema, o palestrante destacou de forma eficaz a importância de compreender e mitigar os riscos cibernéticos, especialmente num ambiente empresarial cada vez mais digitalizado e interconectado. Uma das principais conclusões que pude tirar é a complexidade dos desafios enfrentados pela EDP e empresas como a mesma, dada a sua presença multinacional e a ampla cadeia de valor na indústria de energia. A dependência de prestadores de serviços externos e a necessidade de proteger uma vasta gama de recursos, desde dados pessoais até infraestruturas críticas, tornam as empresas vulneráveis a uma variedade de ameaças cibernéticas.

Em resumo, a palestra ofereceu insights valiosos sobre os desafios e estratégias em cibersegurança. Com uma compreensão clara desses desafios e uma postura de vigilância contínua, as empresas podem fortalecer a sua resiliência contra ameaças cibernéticas e proteger os seus ativos críticos com eficácia.

## REFERÊNCIAS

(Wikipédia, s.d.)

(EDP, 2024)

ANEXOS