**Jogo MOOCSEG**



**pMOOC Segurança da Informação: Teoria aliada à prática**

Melo, William da Silva

M528m pMOOC Segurança da Informação: teoria aliada à prática: jogo MOOCSEG/ William da Silva Melo.

II, 8f.

Produto Educacional parte da dissertação intitulada “Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação” apresentada ao Programa de Pós-Graduação em Educação Profissional e Tecnológica ofertado pelo Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF Sertão PE) / Campus Salgueiro, Salgueiro, PE, 2020.

* + 1. Segurança da Informação 2. pMOOC 3. MOOCSEG – Jogo educativo I. Título

CDD 371.33

Ficha Catalográfica Elaborada pela Bibliotecária Naira Michelle Alves Pereira CRB 4/1891

**SUMÁRIO**

1. **APRESENTAÇÃO.............................................................................................3**
2. **MANUAL MOOCSEG.......................................................................................4**
3. **BARALHO MOOCSEG.....................................................................................5**

**APRESENTAÇÃO**

Como produto educacional foi elaborado um jogo de cartas denominado MOOCSEG, trata-se de um dos elementos que compõe a sequência didática elaborada na pesquisa: Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação, foi criado o jogo de cartas denominado MOOCSEG. O jogo em questão foi aplicado presencialmente, em grupo com as turmas do Ensino Médio Integrado ao técnico de Informática do

O jogo de cartas MOOCSEG foi apresentado pelo mestrando William da Silva Melo, sob orientação de Francisco Kelsen de Oliveira, no programa de Pós Graduação em Educação Profissional e Tecnológica, ofertado pelo Instituto Federal de Educação, Ciências e Tecnologia do Sertão Pernambucano, campus Salgueiro. O mesmo foi concebido para inserir o elemento da gamificação no curso on-line aberto e massivo pMOOC Segurança da Informação: Aliando teoria e prática e pode ser adaptado para outras áreas do conhecimento. Para tal, basta apenas que sejam adaptados os pares de cartas que estão disponíveis na sessão Baralho MOOCSEG, as regras do jogo podem ser consultadas na sessão manual MOOCSEG.

**MANUAL MOOCSEG**

**Material necessário**

* 2 baralhos MOOCSEG
* 2 fitas adesivas
* Cronômetro
* Brinde (Prêmio)

**Regras**

* O professor ou mediador deve dividir a turma em dois grupos
* O baralho deve ser misturado, cada grupo receberá 15 pares de cartas contendo conceito – definição, esses conceitos estão relacionados aos princípios da segurança da informação e aos códigos maliciosos conforme ilustra a sessão baralho MOOCSEG.
* Não é permitida consulta
* Os grupos tem quinze minutos para discutir entre si o que consideravam ser os pares de cartas corretos
* Os grupos devem colar as cartas no quadro entregando suas respostas
* Cada par de cartas correto equivale a um ponto.
* Depois que o tempo acaba os grupos não podem entregar as respostas
* É feita a conferência da pontuação de cada grupo
* Enquanto é feita a conferência o professor ou mediador pode discorrer sobre os pares de cartas dando exemplos e relacionando os conceitos com situações reais amplamente divulgadas pela mídia.
* O grupo que que fez mais pontos vence o desafio e ganha o brinde.

**BARALHO MOOCSEG**

|  |  |  |
| --- | --- | --- |
| **Vulnerabilidade** | **Ameaça** | **Risco** |
| Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque | Possível evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso | Possível evento potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante |
| **Vírus** | **Worm** | **Bot** |
| Programa ou parte de um programa de computador, normalmente malicioso, que permite inserir as seguintes cópias e se tornar parte de outros programas e arquivos. | Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. | Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente |
| **Spyware** | **Backdoor** | **Trojan** |
| Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros | Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim | Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. |
| **Ransomware** | **Phishing** | **Sniffing** |
| Código malicioso que exige o pagamento de um resgate para recuperar a informação do usuário | Golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social | Inspeciona os dados trafegados em redes de computadores |
| **Adware** | **Screenlogger** | **Keylogger** |
| Spyware projetado especificamente para apresentar propagandas | Spyware capaz de armazenar a posição do cursor e a tela apresentada no monitor | Spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador |