UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE	
FICHA DE EXPECTATIVA DE RESPOSTA DA PROVA ESCRITA	
Edital nº:	**010/2018-PROGESP**
Carreira:	(**X**) MAGISTÉRIO SUPERIOR ( ) MAGISTÉRIO EBTT
Unidade Acadêmica:	**Instituto Metrópole Digital (IMD)**
Área de Conhecimento:	**SEGURANÇA DA INFORMAÇÃO**

CRITÉRIOS DE AVALIAÇÃO PARA TODAS AS QUESTÕES DISCURSIVAS

- Clareza e propriedade no uso da linguagem;
- Coerência e coesão textual;
- Domínio dos conteúdos, evidenciando a compreensão dos temas objeto da prova;
- Domínio e precisão no uso de conceitos;
- Coerência no desenvolvimento das ideias e capacidade argumentativa.

QUESTÃO 1: **TEMA 3. SSL/TLS, IPSec e VPN. Valor. (0,00 a 5,00 pts)**

Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Conceitos, objetivos, arquitetura e funcionamento do SSL/TLS; Conceitos, objetivos, arquitetura e funcionamento do IPSec; Conceitos, objetivos, arquitetura e funcionamento de VPNs; Comparação entre os três tópicos mencionados.

QUESTÃO 2: **TEMA 5. Segurança em Sistemas Operacionais: mecanismos de controle de acesso, mecanismos de autenticação, mecanismos de proteção de memória e segurança de máquinas virtuais. Valor (0,00 a 5,00 pts)**

Espera-se que o candidato seja capaz de abordar os seguintes tópicos em cada um dos quatro itens mencionados no enunciado.

Mecanismos de controle de acesso: Matriz, ACL, *capabilities*, RBAC; Estrutura baseada em anéis; Monitor de referência; Exemplo em S.O. moderno: Controle de acesso Unix ou Windows, SELinux.

Mecanismos de autenticação: Conceitos básicos; Princípios de autenticação: o que você sabe, o que você tem, o que você é; Modelos de autenticação: tradicional (local), centralizado, federado, centrado no usuário; Autenticação local vs Autenticação remota; Exemplos de tecnologias: PAM, *Kerberos* ou RADIUS.

Mecanismos de proteção de memória: Organização da memória: segmentos; Ataques à memória - Programação baseada em retorno; *NX-Stack* e suas limitações; W^X (*Either Writable or Executable Memory*); Implementações: PaX (Linux) e NX Bit (Windows) e outros; Limitações; *Stack Data Protection*: *Canaries*; AAAS (*ASCII Armored Address Space*), ASLR (*Address Space Layout Randomization*); Proteções para a *Heap*: proteções para as operações *free()* e *unlink()*.

Segurança de máquinas virtuais: Conceitos básicos sobre virtualização: tipo I (nativa), tipo II (hospedada), *Hypervisor*, tradução dinâmica, para-virtualização; Propriedades de segurança: Completude, Isolamento, Transparência; Vulnerabilidades de virtualização: Mecanismos de segurança baseado em introspecção, em proteção e recuperação.

-------- TEMAS NÃO SORTEADOS --------

TEMA 1. Arquitetura, protocolos e algoritmos para autenticação e autorização, auditoria.
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Conceitos básicos sobre a tríade AAA (*Authentication, Authorization and Accounting*); Princípios de autenticação: o que você sabe, o que você tem, o que você é; Modelos de autenticação: tradicional (local), centralizado, federado, centrado no usuário; Protocolos de autenticação; Princípios de controle de acesso; Políticas de controle de acesso (MAC, DAC, RBAC, ABAC); Arquitetura de referência para sistemas de autorização (PAP, PEP, PDP, PIP); Princípios, objetivos e desafios de auditoria.

TEMA 2. Criptografia simétrica e assimétrica e suas aplicações; funções hash e assinatura digital; PKI e Certificados Digitais.
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Criptosistemas simétricos: componentes, cifra de bloco, DES e AES; Criptosistemas assimétricos: RSA; Infraestrutura de Chave Pública (PKI); Problemas e técnicas para a distribuição de chaves: Diffie-Hellman, Elgamal e Certificados Digitais (padrão X.509); Métodos para assinatura digital; Funções hash e suas utilizações.

TEMA 4. firewalls, IDS e IPS.
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Conceitos, objetivos, arquitetura e funcionamento de firewalls; Conceitos, objetivos, arquitetura, funcionamento de IDS e IPS, e sua integração com firewalls; Arquiteturas de implementação destes componentes em rede e seu impacto na segurança da rede.

TEMA 6. Segurança em redes sem fios: WEP, WPA, WPA2, 802.1X e 802.11i.
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Wired Equivalency Privacy (WEP) - encriptação com RC4 e suas vulnerabilidades; Especificação IEEE 802.11i - uso de AES e uma arquitetura de componentes 802.1X; Wireless Protected Access (WPA) - encriptação com Temporal Key Integrity Protocol (TKIP) e autenticação com IEEE 802.1X(EAPoL); IEEE 802.11i (WPA2) - suporte a diferentes protocolos de privacidade (TKIP - RC4, CCMP - AES) e autenticação (RSN - IEEE 802.1X, PSK). Fragilidades do protocolo WPA2 (*KRACK Attacks*).

TEMA 7. Princípios de perícia e análise forense computacional.
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Problemas atuais com Evidências Digitais; Introdução à Metodologia de Computação Forense; Limites legais e éticos relativos à investigação e auditoria; Normas e legislação; Sistemas Numéricos e Unidades de Volume, Codificação de Caracteres e *Hash*; Partições e Sistemas de Arquivos; Cadeia de Custódia;

TEMA 8. Gestão da Segurança: Política de Segurança, padrões de segurança (ISO 27001, ISO 27002, ISO 27005 e ISO 15408) e o Marco Civil da Internet (Lei N° 12.965/14).
Espera-se que o candidato seja capaz de dissertar sobre os seguintes tópicos: Definição e implementação de políticas de segurança da informação; Aspectos de segurança da informação conforme definido pelas normas ISO 27001, ISO 27002, ISO 27005 e ISO 15408; Marco Civil da Internet: neutralidade da rede e suas Implicações para segurança da informação.

Assinatura dos Membros da Comissão	1º membro (Presidente): 2º membro: 3º membro: