UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE	
FICHA DE EXPECTATIVA DE RESPOSTA DA PROVA ESCRITA	
Edital nº:	**035/2017-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 7. Princípios de perícia e análise forense computacional. Valor. (0,00 a 5,00 pts)**

Espera-se que o candidato seja capaz de dissertar sobre os seguintes temas: 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* e Partições e Sistemas de Arquivos; Cadeia de Custódia;

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*: protegendo operações de *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.

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