- Nesta prova, faça o que se pede, usando, caso deseje, o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado.
- Na **Folha de Texto Definitivo**, a presença de qualquer marca identificadora no espaço destinado à transcrição do texto definitivo acarretará a anulação da sua prova discursiva.
- Ao domínio do conteúdo serão atribuídos até **20,00 pontos**, dos quais até **1,00 ponto** será atribuído ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado).

-- PROVA DISCURSIVA –

Em março de 2023, os sistemas SCADA de uma usina geradora e distribuidora de energia elétrica foram paralisados por três horas, o que afetou diretamente a distribuição de energia em três grandes cidades da região Nordeste do Brasil. Após a constatação de que a interrupção havia sido causada pela execução de um arquivo binário malicioso em uma estação crítica, o qual se caracterizava por polimorfismo, execução *fileless* e forte ofuscação, a Polícia Federal foi acionada, tendo sido o setor de informática forense o responsável pela resposta ao incidente, ao qual coube identificar o comportamento do *malware* e indicar possíveis ligações com ameaças persistentes avançadas (APT), além de buscar identificadores de autoria do ataque.

Considerando a situação narrada, redija um texto dissertativo em atendimento ao que se pede a seguir.

1 Explique as quatro principais técnicas antiforenses que grupos criminosos utilizam na criação de *malwares*. [**valor: 6,00 pontos**]

2 Mencione o papel de métodos de análise como *debuggers*, descompiladores, *sandboxes* e análise de código Assembly no exame técnico. [**valor: 8,00 pontos**]

3 Descreva um processo de utilização dessas soluções e suas principais funções. [**valor: 5,00 pontos**]

RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	