PROVA DISCURSIVA – GESTOR DE TECNOLOGIA DA INFORMAÇÃO

CANDIDATO(A): _____	**INSCRIÇÃO: _____**

ESTUDO DE CASO

Valor: 100 pontos

A Câmara Municipal de São Miguel do Guaporé utiliza ambiente tecnológico integrado para execução de atividades administrativas e legislativas, compreendendo sistemas de protocolo, recursos humanos, gestão documental, serviços internos, armazenamento de arquivos e publicação de informações institucionais.

Em uma manhã de expediente, diversos servidores relataram indisponibilidade simultânea de sistemas e arquivos compartilhados. A equipe técnica constatou que grande quantidade de arquivos armazenados em servidor institucional havia sido criptografada e que uma mensagem exigindo pagamento para sua recuperação estava disponível no ambiente afetado.

Na análise inicial, foram identificados registros de acesso remoto realizado durante a madrugada por credencial com privilégios administrativos. A mesma credencial era utilizada, em situações distintas, por mais de um integrante da equipe técnica e também havia sido disponibilizada à empresa contratada para suporte de determinados sistemas. O acesso remoto não utilizava mecanismo adicional de autenticação.

Verificou-se ainda que os backups automáticos eram armazenados em equipamento conectado permanentemente à mesma rede dos servidores afetados. As cópias mais recentes apresentavam indícios de comprometimento, enquanto a última cópia mantida em ambiente distinto havia sido realizada vários dias antes e não havia registro recente de teste de restauração.

Durante a apuração, também foram observadas conexões atípicas envolvendo volume significativo de dados. Não era possível, naquele momento, confirmar se houve transferência externa de arquivos, porém o ambiente afetado continha documentos com dados pessoais de servidores, fornecedores e terceiros.

A empresa responsável pelo suporte técnico recomendou a reinstalação imediata dos servidores e a restauração da cópia disponível, a fim de reduzir o período de indisponibilidade. Entretanto, não havia sido concluída a preservação dos registros técnicos necessários à análise do incidente. Também se constatou que a Câmara não possuía procedimento formal atualizado para resposta a incidentes, nem parâmetros previamente definidos de tempo e ponto aceitáveis para recuperação dos serviços.

A Presidência solicitou ao Gestor de Tecnologia da Informação manifestação técnica e adoção das providências necessárias para restabelecer os serviços essenciais com segurança, preservar as informações institucionais e reduzir o risco de recorrência.

Na condição de Gestor de Tecnologia da Informação, analise a situação apresentada e indique, de forma fundamentada, as medidas técnicas, administrativas e de governança que deverão ser adotadas para tratamento do incidente, recuperação dos serviços e aperfeiçoamento dos controles de Tecnologia da Informação da Câmara Municipal.

RESPOSTA

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
31
32
33
34
35
36
37
38
39
40
41

42

43

44

45

46

47

48

49

50

51

52