

## CONCURSO PÚBLICO – SDS/PE

### CARGO 11: PERITO CRIMINAL ÁREA 7: CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO OU SISTEMAS DE INFORMAÇÃO

#### PROVA DISCURSIVA – TEXTO DISSERTATIVO

Aplicação: 19/6/2016

### PADRÃO DE RESPOSTA

Em linhas gerais, espera-se do candidato resposta que contemple as seguintes informações, ainda que a ordem na descrição dos habilitadores seja diversa da apresentada.

**1** Define-se habilitador como uma série de fatores que, individualmente ou em conjunto, influencia o funcionamento de algo — no caso, da governança e da gestão corporativas da TI. Os habilitadores são orientados pela cascata de objetivos, ou seja, objetivos de TI em níveis mais alto definem o que os diferentes habilitadores deverão alcançar.

**2** Nomes e definição dos sete habilitadores: (1) princípios, políticas e modelos — são veículos para a tradução do comportamento desejado em orientações práticas para a gestão diária; (2) processos — descrevem um conjunto organizado de práticas e atividades para o atingimento de determinados objetivos e produzem um conjunto de resultados em apoio ao atingimento geral dos objetivos de TI; (3) estruturas organizacionais — são as principais entidades de tomada de decisão da organização; (4) cultura, ética e comportamento (das pessoas e da organização) — conjunto de comportamentos individuais e coletivos de cada organização; (5) informação — permeia qualquer organização e inclui todas as informações produzidas e usadas pela organização, sendo necessária para mantê-la em funcionamento e bem governada, mas, no nível operacional, a informação por si só é, muitas vezes, o principal produto da organização; (6) serviços, infraestrutura e aplicativos — incluem a infraestrutura, a tecnologia e os aplicativos que fornecem à organização o processamento e os serviços de TI; (7) pessoas, habilidades e competências — estão associadas às pessoas e são necessárias para a conclusão bem-sucedida de todas as atividades e para a tomada de decisões corretas e de medidas corretivas.

## CONCURSO PÚBLICO – SDS/PE

### CARGO 11: PERITO CRIMINAL ÁREA 7: CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO OU SISTEMAS DE INFORMAÇÃO

#### PROVA DISCURSIVA – ESTUDO DE CASO

Aplicação: 19/6/2016

### PADRÃO DE RESPOSTA

Espera-se que, para resolver o caso, o candidato contemple em seu texto, em linhas gerais, as informações a seguir.

O *firewall* da rede de computadores da organização deveria estar configurado de maneira restritiva para permitir que o acesso externo à rede fosse realizado somente por meio das portas respectivas para os serviços SMTP (*mail*) e SMTPS (*mail seguro*). Os clientes de correio eletrônico deveriam utilizar o protocolo POP3S ou IMAPS para receber suas mensagens, garantindo-se, assim, que as mensagens, ao serem trafegadas na rede, estivessem protegidas por criptografia. O *firewall* deveria ficar restrito a esses clientes e às portas para POP3S e IMAPS.

Já que o ambiente possui servidor Windows 2012 R2, deveria existir um serviço de Active Directory (AD) nesse ambiente, o que permitiria que tanto os usuários quanto os computadores da rede pudessem ser autenticados no serviço AD. Para a atualização de segurança, o serviço Windows Update deveria estar configurado nas estações Windows 7 e nos servidores de rede. Como função mais avançada, poderia ser utilizado o serviço WSUS para atualizações de redes corporativas.

O OpenLDAP, que é um serviço de autenticação de usuários, pode ser removido da rede se for instalado o serviço de AD no Windows 2012 R2, porque se torna redundante na rede, gerando dois serviços com a mesma finalidade. Assim, por questões de integração de soluções de rede, já que o AD é integrado nativamente ao Windows 2012 R2 e o Windows 7 é compatível com esse serviço, o OpenLDAP pode ser removido, sem prejuízo para a autenticação dos usuários.

Como o *switch* é gerenciável, poderiam ser criados três segmentos de rede, conforme a necessidade de uma DMZ. Nesse caso, o *firewall* deveria ter três interfaces de rede para serem ligadas a três VLANs distintas, que devem ser criadas, sendo cada interface do *firewall* ligada em uma VLAN diferente para roteamento entre as VLANs. A título de exemplo, poderia ser criada uma VLAN externa (Internet), uma VLAN interna (rede local com computadores clientes e serviços de autenticação) e uma VLAN para serviços de Internet (DMZ/*email*, no caso em questão).