CONCURSO FIOCRUZ 2014

CT1368

Tecnologia da Informação com foco em Segurança da Informação

Tecnologista em Saúde Pública

Prova Objetiva

FUNDAÇÃO DOM CINTRA

Conhecimentos Específicos na Área de Atuação

01. O sistema binário é aquele que melhor representa os sinais elétricos no interior dos componentes computacionais. Em uma representação binária de números inteiros com complemento de 1, o módulo do número 00100101 em decimal é:

(A) -39.
(B) 38.
(C) 37.
(D) 39.
(E) -37.

02. A soma de 11110101 e 10000000 produz o seguinte resultado decimal:

(A) 377.
(B) 367.
(C) 387.
(D) 383.
(E) 373.

03. O processador precisa escalonar a execução de processos; por isso esses processos encontram-se em diferentes estados a cada momento. Os estados possíveis para um processo seriam:

(A) executando, pronto, bloqueado.
(B) iniciando, executando, encerrando.
(C) iniciando, pronto, encerrando.
(D) executando, encerrando, bloqueado.
(E) pronto, iniciando, encerrando.

04. As chamadas ao sistema operacional podem ser feitas, por exemplo, com a instrução Assembly INT <número da interrupção>, passando parâmetros através de registradores como AL e AH. O objetivo dessas chamadas é permitir:

(A) a interrupção de processos rodando no sistema operacional.
(B) às aplicações utilizarem funções intrínsecas ao sistemas operacional.
(C) a identificação e chamada de um processo não escalonado.
(D) a identificação e chamada de um processo escalonado.
(E) a chamada paralela e interruptiva de processos, escalonados ou não.

05. O escalonador do sistema operacional pode utilizar diferentes mecanismos de escalonamento de processos. Entre eles podemos citar:

(A) Preemptivo, Não preemptivo, e Bubble Sort.
(B) Árvore Binária, Round Robin, e FIFO.
(C) SJF, Preemptivo e Árvore Binária.
(D) FIFO, SJF e Round Robin.
(E) Não preemptivo, Preemptivo, e Assimétrico.

06. Quando cada processo ativo está dependendo de um evento que outro processo causará, esse fenômeno é chamado de:

(A) referência circular.
(B) deadlock.
(C) recursividade de processo.
(D) espiral de processo.
(E) horizonte circular.

07. O protocolo HTTPS é na verdade uma implementação específica do protocolo HTTP. A diferença é que o HTTPS implementa uma camada de segurança baseada em:

(A) SSL/TLS.
(B) PPP/SSL.
(C) TKIP/WPA.
(D) WPA/PSK.
(E) AES/WEP.

08. O modelo OSI estrutura conceitualmente os protocolos de comunicação em uma rede de computadores. Para esse modelo, o QoS (Quality of Service) é tratado pela camada de:

(A) enlace.
(B) rede.
(C) transporte.
(D) sessão.
(E) apresentação.

09. O TCP/IP é um pacote de protocolos s serviços, entre os quais podem ser destacados os seguintes:

(A) TCP, IPX, UDP, NAT, e TELNET.
(B) TCP, IPX, SPX, ICMP, e WINS.
(C) TCP, IP, UDP, ICMP, e TELNET.
(D) TCP, IPX, SPX, DNS, e IGMP.
(E) TCP, IPX, SPX, Token, e Netbeui.

10. As linguagens regulares de programação são linguagens formais finitas geradas por gramáticas. Essas linguagens são representadas com forte sustentação:

(A) algorítmica.
(B) simbológica.
(C) gramática do idioma inglês.
(D) gramática do idioma português.
(E) matemática.

11. Dito em termos simples um compilador é:

(A) um programa que transforma um conjunto de comandos em linguagem de máquina, que é armazenada e executada pelo computador.
(B) um programa que transforma uma gramática em uma linguagem, e uma linguagem em executável.
(C) um programa que executa as funcionalidade de um sistema desenvolvido em uma linguagem.
(D) um programa que interpreta um conjunto de comandos em linguagem de máquina, que é executada pelo computador.
(E) um programa que anexa diversos programas, compilando-os em um cluster executável.

12. Uma linguagem de programação de alto nível é aquela que:

(A) executa em equipamentos de alto custo operacional.
(B) exige elevado conhecimento e experiência do programador.
(C) independe de humanos, sendo fácil de compreender por dispositivos.
(D) executam em equipamentos de missão crítica.
(E) independe do dispositivo, sendo fácil de compreender por humanos.

13. Em determinada organização, um processo devidamente protocolado em sistema de informação apropriado é extraviado. Isso configura primariamente uma quebra de:

(A) autenticidade e legalidade.
(B) disponibilidade e confidencialidade.
(C) confidencialidade e autenticidade.
(D) legalidade e integridade.
(E) integridade e autenticidade.

14. Em determinada organização, a empresa descobre que os dados dos colaboradores sofreram alterações aleatórias após um problema de queda de energia no datacenter. Esse incidente configura uma quebra de:

(A) confidencialidade.
(B) legalidade.
(C) disponibilidade.
(D) autenticidade.
(E) integridade.

15. Os comandos de sistemas gerenciadores de banco de dados podem ser classificados basicamente em dois conjuntos:

(A) DDL e XML.
(B) DDL e DML.
(C) XML e DML.
(D) DES e DDL.
(E) XML e DES.

16. Os autores da teoria relacional propuseram um conjunto de regras que se aplicam a bancos de dados distribuídos. Entre essas regras podem ser citadas:

(A) autonomia local, operação contínua, independência de rede e independência de SGDB.
(B) autonomia transacional, operação relacional, independência de rede e independência de SGDB.
(C) autonomia local, operação contínua, independência de dados e independência de SGDB.
(D) autonomia transacional, operação contínua, independência de rede e independência de software.
(E) autonomia entre dados, operação contínua, independência de rede e independência de SGDB.

17. Sistemas de banco de dados de alta disponibilidade podem ser uma exigência do negócio de uma organização, o que será determinado pela análise de risco. Os elementos para medição de disponibilidade de um sistema de banco de dados seriam:

(A) MTTR e DP.
(B) FIT e DP.
(C) MTBF e MTR.
(D) MTR e DP.
(E) MTBF e MTTR.

18. Considerando o ITIL v3, o Service Design deve ser aplicado a:

(A) serviços novos.
(B) serviços de segundo nível.
(C) serviços existentes e serviços novos.
(D) serviços de terceiro nível.
(E) serviços existentes.

19. De acordo com o ITIL v3, um importante tema tratado na Transição de serviços é:

(A) redução do risco.
(B) aumento do ROI.
(C) planejamento.
(D) service desk.
(E) PDCA.

20. O processo de melhoria contínua dos serviços de TI, conforme recomendado pelo ITIL v3, depende da:

(A) instalação de softwares de melhoria contínua.
(B) alinhamento estratégico.
(C) sistema integrado da Qualidade.
(D) coleta anterior de informações e indicadores do sistema.
(E) clima organizacional positivo.

Conhecimentos Específicos no Perfil

21. Um incidente de segurança da informação é uma ocorrência em que uma das dimensões de segurança são quebradas, afetando de algum modo o negócio da organização, ou seja, gerando um impacto ou grau de prejuízo. Podemos dizer que um incidente de segurança da informação é decorrente de:

(A) uma vulnerabilidade que produz uma ameaça para o ativo de informação.
(B) um ativo de informação que contém uma ameaça suscetível a uma vulnerabilidade.
(C) uma ameaça que gera impacto na vulnerabilidade de um ativo de informação.
(D) uma ameaça que explora uma vulnerabilidade do ativo de informação.
(E) uma ameaça que produz uma vulnerabilidade para o ativo de informação.

22. Os ativos de informação podem ser classificados em:

(A) tecnologias, ambientes, operações e processos.
(B) tecnologias, pessoas, processos e ambientes.
(C) processos, equipamentos, tecnologias e ambientes.
(D) operações, equipamentos, tecnologias e pessoas.
(E) pessoas, operações, equipamentos, e procedimentos.

23. A área de segurança da informação trabalha fundamentalmente para tratar as vulnerabilidades dos ativos de informação, reduzindo assim os riscos de segurança da informação. Assim, esses esforços devem abranger:

(A) tecnologias de informação, recursos humanos, processos de negócio e estrutura física da organização.
(B) tecnologias de informação, sistemas de informação, redes de computadores e bancos de dados.
(C) cabeamento de rede, roteadores, redes sem fio e processos de negócio.
(D) estrutura física da organização, recursos humanos, patrimônio e redes de computadores.
(E) redes de computadores, bancos de dados, cabos de rede e processos de negócio.

24. O objetivo da gestão de riscos é identificar os riscos em segurança da informação existentes na organização. Cada risco identificado poderá ser tratado da seguinte forma:

(A) transferir, ignorar, aceitar, ou reduzir.
(B) reduzir, aceitar, tratar, ou evitar.
(C) aceitar, evitar, ignorar, ou reduzir.
(D) transferir, tratar, evitar, ou ignorar.
(E) evitar, transferir, reduzir, ou aceitar.

25. A gestão de riscos traz diversos benefícios para a organização, mas o sucesso dessa gestão dependerá da eficácia de sua estrutura de gestão. A estrutura de gestão de riscos conta com os seguintes componentes:

(A) mandato e comprometimento, concepção da estrutura, avaliação dos riscos, implementação da gestão de riscos, e monitoramento e análise crítica da estrutura.
(B) mandato e comprometimento, concepção da estrutura, implementação da gestão de riscos, monitoramento e análise crítica da estrutura, e melhoria contínua.
(C) concepção da estrutura, implementação da gestão de riscos, monitoramento e análise crítica da estrutura, planejamento da melhoria, e melhoria contínua.
(D) projeto de gestão de riscos, concepção da estrutura, implementação da gestão de riscos, monitoramento e análise crítica da estrutura, e planejamento da melhoria.
(E) projeto de gestão de riscos, mandato e comprometimento, monitoramento e análise crítica da estrutura, planejamento da melhoria, e melhoria contínua.

26. O processo de gestão de riscos contém o processo de avaliação de riscos, cujo objetivo é produzir uma lista com todos os possíveis eventos que poderiam representar risco para a organização. O processo de avaliação de riscos é composto das seguintes atividades:

(A) identificar riscos, verificar riscos e tratar riscos.
(B) identificar riscos, analisar riscos e tratar riscos.
(C) identificar riscos, analisar riscos e avaliar riscos.
(D) identificar riscos, analisar riscos e dimensionar riscos.
(E) analisar riscos, verificar riscos e tratar riscos.

27. A política de segurança da informação é um conjunto de orientações que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação. Essas orientações são estruturadas na forma de:

(A) diretrizes que orientam as normas, que orientam os procedimentos.
(B) diretrizes que orientam as normas, que orientam as regras.
(C) normas que orientam as regras, que orientam os procedimentos.
(D) normas que orientam procedimentos, que orientam regras.
(E) padrões que orientam as diretrizes, que orientam as normas.

28. A política de segurança da informação precisa preservar os direitos e respeitar os deveres previamente estabelecidos por mecanismos legais e regulatórios. Algumas das questões importantes nesse sentido são:

(A) aderir à legislação vigente, aderir à ISO 9.000, preservar os bancos de dados, e manter a conformidade legal dos sistemas de informação.
(B) aderir à legislação vigente, aderir à ISO 14.000, preservar os registros organizacionais, e manter a conformidade legal dos sistemas de informação.
(C) aderir à legislação vigente, garantir os direitos de propriedade intelectual, preservar os registros organizacionais, e manter a conformidade legal dos sistemas de informação.
(D) aderir à legislação vigente, garantir os direitos de comunicação aberta, preservar os registros organizacionais, e manter a conformidade legal dos sistemas de informação.
(E) aderir à legislação vigente, garantir o uso de software livre, preservar os bancos de dados, e manter a conformidade legal dos sistemas de informação.

29. O principal objetivo da política de segurança da informação é estabelecer um padrão de comportamento que seja conhecido por todos e que sirva de base para decisões da alta direção em assuntos relacionados com segurança da informação. Essa política precisa considerar:

(A) o sistema de gestão de segurança, o monitoramento e a auditoria, e estar alinhada com esses elementos.
(B) a estrutura física, as operações, e os acessos lógicos, e estar alinhada com esses elementos.
(C) os equipamentos, infraestrutura de rede e sistemas de informação, e estar alinhada com esses elementos.
(D) os colaboradores, os clientes e os fornecedores da organização, e estar alinhada com esses elementos.
(E) a missão, a visão, e o modelo estratégico da organização, e estar alinhada com esses elementos.

30. A classificação da informação é fundamental para que as organizações possam direcionar os seus recursos para sistemas de segurança. O objetivo da classificação da informação é tratar a informação de acordo com:

(A) seu valor, requisitos legais, grau de sensibilidade, criticidade e necessidade de compartilhamento.
(B) sua estrutura, tamanho, e espaço de armazenamento.
(C) sua fonte de produção, seu uso no processo organizacional, e seu objetivo final.
(D) sua dimensão estratégica, valor comercial, impacto para o cliente, e uso operacional.
(E) seu valor comercial, sua estrutura, sua fonte de produção e sua dimensão estratégica.

31. A criptografia é um importante controle para a segurança da informação, mas assim como os demais controles, sua aplicação deve ser um resultado da análise de risco. A maior vulnerabilidade da utilização de chaves simétricas para criptografia reside no fato de que a chave:

(A) precisa ser gravada com a mensagem, e isso torna difícil a leitura.
(B) é padronizada, e isso impossibilita alterações.
(C) é grande, e isso demanda muito processamento.
(D) é pequena, e isso oferece pouca segurança.
(E) precisa ser compartilhada, e isso possibilita extravio.

32. A segurança física e do ambiente é uma importante ferramenta de segurança da informação. O objetivo do estabelecimento de perímetros é:

(A) impedir o acesso à determinado ativo de informação.
(B) dificultar o acesso à determinada funcionalidade de um sistema de informação.
(C) dificultar progressivamente o acesso à determinado ativo de informação.
(D) impedir o acesso à determinada funcionalidade de um sistema de informação.
(E) desviar o acesso de determinado ativo de informação.

33. O inventário de ativos de informação é um mecanismo fundamental em um sistema de segurança da informação. Um dos objetivos de um inventário de ativos é:

(A) manter a segurança dos recursos de processamento da informação.
(B) prevenir o acesso não autorizado aos ativos da organização.
(C) assegurar que a informação receba um nível adequado de proteção.
(D) alcançar e manter a proteção adequada dos ativos da organização.
(E) garantir a operação segura e correta dos ativos da organização.

34. O plano de continuidade do negócio tem como objetivo impedir a interrupção dos processos de negócio mesmo nos casos de incidente de segurança da informação. Um plano de continuidade é acionando quando um incidente de segurança da informação interrompe um processo de negócio por um tempo:

(A) mínimo suportado pelo negócio em questão.
(B) superior ao máximo suportado pelo negócio em questão.
(C) médio suportado pelo negócio em questão.
(D) maior do que o suportado pelo cliente do negócio em questão.
(E) superior ao horário de expediente da organização.

35. O impacto se refere a quanto prejuízo um incidente de segurança da informação pode gerar. É possível afirmar que o impacto poderá ser medido com base:

(A) no grau da ameaça e no grau de vulnerabilidade do processo de negócio.
(B) na relevância do ativo para um serviço e na relevância do serviço para o processo de negócio.
(C) na probabilidade do incidente de segurança e na ameaça ao processo de negócio.
(D) no grau de ameaça e no grau de prejuízo causado ao processo de negócio.
(E) na relevância das tecnologias, pessoas e ambientes.

36. Uma importante estratégia de continuidade de negócio é ter um site backup da estrutura computacional da organização. Um site morno (warm site) é uma estrutura que:

(A) apresenta condições similares à estrutura principal de computação da organização, e que pode ser operacionalizada imediatamente após a ocorrência de um desastre.
(B) já conta com espaço, energia e link de dados, e que pode receber todos os equipamentos da estrutura principal de computação da organização logo após a ocorrência de um desastre.
(C) apresenta condições similares à estrutura principal de computação da organização, e que pode ser operacionalizada com algum tempo e esforço após a ocorrência de um desastre.
(D) apresenta condições superiores à estrutura principal de computação da organização, e que opera a maior parte do tempo como site principal da organização, evitando tempo e esforço para operacionalização após a ocorrência de um desastre.
(E) apresenta condições idênticas à estrutura principal de computação da organização, e que opera a metade do tempo como site principal da organização, evitando tempo e esforço para operacionalização após a ocorrência de um desastre.

37. Apesar da aplicação das recomendações da disciplina de segurança da informação, ainda é possível a ocorrência de incidentes de segurança da informação. Nesses casos, é fundamental que a organização responda a cada incidente de segurança da informação imediatamente. A resposta ao incidente de segurança é composta dos seguintes passos:

(A) 1) preparação, 2) identificação, 3) contenção, 4) erradicação, 5) recuperação e 6) lições aprendidas.
(B) 1) reparação, 2) identificação, 3) transferência, 4) erradicação, 5) recuperação e 6) lições aprendidas.
(C) 1) contenção, 2) preparação, 3) comunicação, 4) erradicação, 5) recuperação e 6) lições aprendidas.
(D) 1) erradicação, 2) preparação, 3) identificação, 4) contenção, e 6) controle.
(E) 1) contenção, 2) erradicação, 3) preparação, 4) identificação, 5) controle e 6) lições aprendidas.

38. O controle de acesso físico é amplamente utilizado em um sistema de segurança da informação. Uma fragilidade desse tipo de controle são as ocorrências de incêndio porque:

(A) os equipamentos são destruídos.
(B) os dados são perdidos.
(C) as pessoas podem perder seus cartões magnéticos.
(D) o acesso físico precisa ser liberado a todos.
(E) a fumaça impede a visualização dos controles de acesso.

39. As pessoas são o elemento central de um sistema de segurança da informação. Podemos afirmar que a organização é, na verdade, o conjunto de pessoas que nela trabalham. Durante a fase de seleção de pessoal, uma verificação de segurança da informação para o candidato seria checar:

(A) eventuais processos trabalhistas.
(B) capacidade de relacionamento interpessoal.
(C) nível de organização e coordenação de tarefas.
(D) capacidade de gestão de projetos.
(E) referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal.

40. Quando um colaborador é desligado ou realocado em outra função, é importante que sejam tomadas ações referentes à segurança da informação. Entre essas ações estão:

(A) bloquear a senha do colaborador depois de um período de transição, alterar senhas de serviços que o colaborador tenha conhecimento imediatamente e reaver imediatamente quaisquer ativos de informação que possam estar na posse do colaborador.
(B) bloquear a senha do colaborador imediatamente, alterar senhas de serviços que o colaborador tenha conhecimento depois de um período de transição e reaver imediatamente quaisquer ativos de informação que possam estar na posse do colaborador.
(C) bloquear a senha do colaborador imediatamente, alterar senhas de serviços que o colaborador tenha conhecimento imediatamente e reaver depois de um período de transição quaisquer ativos de informação que possam estar na posse do colaborador.
(D) bloquear a senha do colaborador imediatamente, alterar senhas de serviços que o colaborador tenha conhecimento imediatamente e reaver imediatamente quaisquer ativos de informação que possam estar na posse do colaborador.
(E) bloquear a senha do colaborador depois de um período de transição, alterar senhas de serviços que o colaborador tenha conhecimento imediatamente e reaver depois de um período de transição quaisquer ativos de informação que possam estar na posse do colaborador.

41. O treinamento para conscientização em segurança da informação deve se realizado por meio de um processo formal de indução concebido para introduzir as políticas e expectativas de segurança da informação da organização, antes que seja dado acesso às informações ou serviços. Devem ser treinados:

(A) funcionários, clientes e fornecedores.
(B) funcionários, clientes e terceiros.
(C) funcionários, fornecedores e terceiros.
(D) clientes, fornecedores e terceiros.
(E) funcionários, fornecedores e auditores.

42. Em um sistema de informação é necessário garantir que as informações que entram nesse sistema sejam confiáveis e corretas. Para isso, poderão ser aplicados os controles de:

(A) dupla entrada, análise periódica de campos-chave da base, inspeção manual de documentos, validação de erros, e plausibilidade de dados.
(B) dupla entrada, análise periódica de campos-chave da base, inspeção biométrica de documentos, validação de erros, e plausibilidade de campos.
(C) dupla entrada, análise atemporal de campos-chave da base, inspeção automática de documentos, validação de erros, e plausibilidade de campos.
(D) dupla entrada, análise periódica de campos-chave da base, inspeção de dados na base, validação de erros, e plausibilidade de campos.
(E) entrada simples, análise periódica de campos-chave da base, inspeção automática de documentos, validação de erros, e plausibilidade de campos.

43. Tipicamente, sistemas e aplicações são construídos no pressuposto de que, tendo sido efetuadas as validações apropriadas, verificações e testes, as saídas estarão sempre corretas. Esse pressuposto:

(A) é válido na maioria dos casos, isto é, sistemas que tenham sido testados adequadamente não produzem dados de saída incorretos.
(B) não é válido na maioria dos casos, isto é, sistemas que tenham sido testados adequadamente ainda produzem dados de saída incorretos.
(C) não é válido para sistemas de missão crítica, isto é, sistemas de missão crítica que tenham sido testados adequadamente ainda produzem dados de saída incorretos.
(D) sempre é válido, isto é, sistemas que tenham sido testados adequadamente não produzem dados de saída incorretos.
(E) nem sempre é válido, isto é, sistemas que tenham sido testados podem ainda produzir dados de saída incorretos sob certas circunstâncias.

44. O uso de senha é o principal mecanismo adotado pelas organizações para conferir acessos a dados e sistemas, e por isso é importante que haja um processo formal de gestão dessas senhas. Um processo desse tipo deve incluir:

(A) solicitação ao usuário que assine uma declaração onde se compromete em manter a confidencialidade de sua senha.
(B) definição de padrões de senha que sejam fáceis de memorizar, o que evitaria a anotação de senhas.
(C) não fornecimento de senhas temporárias, que são inseguras e geralmente compartilhadas.
(D) fornecimento de senhas temporárias padronizadas e compartilhadas por pequenos grupos de colaboradores.
(E) garantia de que as senhas sejam duplicadas de maneira desprotegida para o administrador, evitando que colaboradores bloqueiem dados da organização.

45. Quando o conceito de definição de perímetros é aplicado às redes, isso é realizado através da segregação de redes. Uma forma de segregar redes é a instalação de:

(A) uma bridge entre a rede interna e duas redes internas.
(B) um roteador entre a rede interna e a rede externa.
(C) um switch entre duas redes internas.
(D) um roteador entre duas redes internas.
(E) um firewall entre duas redes internas.

46. O trabalho remoto tem sido adotado por muitas organizações, reduzindo o custo fixo de operação dessas organizações. Para se garantir a proteção apropriada ao local do trabalho remoto, os seguintes aspectos de segurança devem ser levados em consideração:

(A) segurança física, dos termos de conduta, das comunicações, do uso de redes domésticas, e licenciamento de software.
(B) segurança física, do ambiente, das comunicações, do uso de redes domésticas, e seguro de equipamentos.
(C) segurança física, do ambiente, das comunicações, do uso de redes domésticas, e licenciamento de software.
(D) segurança lógica, do ambiente, das comunicações, do uso de redes domésticas, e seguro de equipamentos.
(E) segurança física, do ambiente, da telefonia, do uso de redes corporativas, e licenciamento de software.

47. Os equipamentos que recebem, transformam ou entregam dados são considerados ativos de informação e precisam ser protegidos. Entre os mecanismos de proteção para equipamentos podem ser mencionados:

(A) seguro contra roubo, proteção contra furto, proteção contra raios, e membranas para teclados, e administração do domínio.
(B) seguro contra roubo, proteção contra furto, proteção contra raios, e membranas para teclados, e proteção do usuário.
(C) posicionamento adequado do equipamento, proteção contra furto, garantia estendida, e membranas para teclados.
(D) posicionamento adequado do equipamento, proteção contra furto, proteção contra raios, e membranas para teclados.
(E) posicionamento adequado do equipamento, proteção contra furto, proteção contra raios, e garantia estendida.

48. O cabeamento que suporta o ambiente computacional é vulnerável e precisa ser protegido. Algumas medidas para a proteção do cabeamento são:

(A) cabeamento subterrâneo, marcas de identificação nos cabos, controle de acesso aos cabos de dados, identificação dos usuários, e política de acesso ao cabeamento de dados.
(B) cabeamento subterrâneo, separação entre cabos de energia e de dados, marcas de identificação nos cabos, controle de acesso aos cabos elétricos, e controle de acesso aos cabos de dados.
(C) cabeamento aéreo, marcas de identificação nos cabos, controle de acesso aos cabos de dados, identificação dos usuários, e política de acesso ao cabeamento de dados.
(D) cabeamento aéreo, separação entre cabos de energia e de dados, marcas de identificação nos cabos, controle de acesso aos cabos elétricos, e controle de acesso aos cabos de dados.
(E) cabeamento subterrâneo, separação entre cabos de energia e de dados, identificação dos usuários, controle de acesso aos cabos elétricos, e controle de acesso aos cabos de dados.

49. O código fonte de programas pode ser intencionalmente alterado para, por exemplo, transferir centavos de cada transação financeira para uma determinada conta. São medidas que podem evitar incidentes com código fonte de programas:

(A) registrar cada acesso ao código fonte por cada programador, e cada atualização da biblioteca de código fonte ser previamente autorizada oficialmente.
(B) implementar um controle de acesso biométrico para cada programador, e cada atualização da biblioteca de código fonte ser previamente autorizada oficialmente.
(C) registrar cada acesso ao código fonte por cada programador, e manter o backup dos códigos fontes em site seguro externo.
(D) implementar um controle de acesso biométrico para cada programador, e manter o backup dos códigos fontes em site seguro externo.
(E) manter o backup dos códigos fontes em site seguro externo e instalar câmeras nos principais acessos ao ambiente de programação.

50. Ativos de informação, como computadores, podem eventualmente ser doados após determinado período de uso, quando a organização não tem mais interesse nesses equipamentos. Antes de doar esses equipamentos a empresa deve:

(A) instalar um novo sistema operacional, e se isso não for possível, formatar o disco rígido.
(B) deletar todos os arquivos do computador, e depois esvaziar integralmente a lixeira.
(C) remover todos os aplicativos instalados no computador, e depois esvaziar a lixeira.
(D) formatar as mídias com sobreposição integral, e se isso não for possível, destruir as mídias fisicamente.
(E) formatar as mídias no padrão NTFS, garantindo o uso correto das mesmas sem oferecer riscos.

51. A criptografia simétrica é aquela que utiliza:

(A) uma chave pública para cifrar a mensagem e uma chave privada para decifrar a mensagem.
(B) uma chave para cifrar a mensagem e a mesma chave para decifrar essa mensagem.
(C) uma chave privada para cifrar a mensagem e uma chave pública para decifrar essa mensagem.
(D) uma chave para cifrar a mensagem e uma chave diferente para decifrar essa mensagem.
(E) uma chave pública para cifrar a mensagem e uma chave pública para decifrar a mensagem.

52. Funções de HASH como MD4, e MD5 e SHA-1 são algoritmos matemáticos que criam um código chamado "message digest". Essas funções possibilitam:

(A) manter a chave de cifragem embutida no arquivo.
(B) reduzir o tamanho do arquivo cifrado através do sistema de compactação.
(C) cifrar os direitos de acesso ao arquivo.
(D) integrar diversos arquivos de maneira cifrada e compactada.
(E) determinar se um arquivo foi contaminado por vírus ou corrompido.

53. A aposição de uma assinatura digital em um documento subscrito garante:

(A) a autoria e a confidencialidade do documento.
(B) a imutabilidade lógica e a disponibilidade do documento.
(C) a autoria e a imutabilidade lógica do documento.
(D) a imutabilidade lógica e a visibilidade do documento.
(E) a autoria e visibilidade do documento.

54. Em determinada organização a equipe de infraestrutura fez ajustes nos servidores DNS, implicando em que diversos sistemas de informação ficaram fora do ar. Essa ocorrência é consequência da AUSÊNCIA de:

(A) plano gestão de mudanças.
(B) plano de continuidade do negócio.
(C) plano de contingência.
(D) política de segurança da informação.
(E) capacitação adequada para a equipe de infraestrutura.

55. Quando diferentes computadores em uma rede estão com seus relógios marcando horários diferentes, isso pode proporcionar a ocorrência de diversos incidentes de segurança da informação. Para manter os relógios sincronizados foi desenvolvido o seguinte protocolo:

(A) UDP
(B) TCP
(C) NTP
(D) HTTPS
(E) IPX

56. Uma das táticas utilizadas por invasores de sistemas de informação é não deixar evidências de suas invasões. Para isso eles alteram:

(A) seus nomes.
(B) os registros de LOG.
(C) os bancos de contas.
(D) os bancos de dados.
(E) dados em memória RAM.

57. O Firewal é responsável por:

(A) analisar o tráfego de entrada, bloqueando determinados hosts, protocolos ou portas.
(B) traduzir endereços IP para portas.
(C) analisar o tráfego de saída, bloqueando determinados hosts, protocolos ou portas.
(D) analisar o trafego de entrada/saída da rede, bloqueando determinados hosts, protocolos ou portas.
(E) traduzir endereços de IP e portas para outros endereços IP e portas.

58. O NAT é responsável por:

(A) analisar o tráfego de entrada, bloqueando determinados hosts, protocolos ou portas.
(B) traduzir endereços IP para portas.
(C) analisar o tráfego de saída, bloqueando determinados hosts, protocolos ou portas.
(D) analisar o tráfego de entrada/saída da rede, bloqueando determinados hosts, protocolos ou portas.
(E) traduzir endereços de IP e portas para outros endereços IP e portas.

59. Para que colaboradores de uma organização acessem com segurança os dados na empresa a partir de redes externas WIFI é possível se utilizar a tecnologia VPN. Nesse caso, os dados são encriptados durante a transferência por protocolos tais como:

(A) TCP, IP e UDP.
(B) HTTPS, RTP E DCCP.
(C) Ethernet, 802.11 e HDLC.
(D) HTTP, SMTP e FTP.
(E) IPSec, L2TP e PPTP/MPPE.

60. Ferramentas de IDS analisam utilização de CPU, I/O de disco, uso de memória e atividades dos usuários. O objetivo dessa ferramenta é:

(A) alertar quanto a ação de hackers na rede da organização.
(B) monitorar o uso dos recursos computacionais.
(C) alertar quanto a ação de vírus.
(D) monitorar o uso dos recursos da rede.
(E) determinar a necessidade de ampliação dos recursos computacionais.

INSTRUÇÕES

1. Por motivo de segurança a Fundação Dom Cintra solicita que o candidato transcreva em letra cursiva, em espaço próprio no Cartão de Respostas, a frase abaixo apresentada:

"As melhores coisas da vida, não podem ser vistas nem tocadas, mas sim sentidas pelo coração." (Dalai Lama)

2. Para cada uma das questões da prova objetiva são apresentadas 5 (cinco) alternativas classificadas com as letras (A), (B), (C), (D) e (E), e só uma responde da melhor forma possível ao quesito proposto. Você só deve assinalar UMA RESPOSTA. A marcação de nenhuma ou de mais de uma alternativa anula a questão, MESMO QUE UMA DAS RESPOSTAS SEJA A CORRETA.
3. A duração da prova é de 4 (quatro) horas, considerando, inclusive, a marcação do Cartão de Respostas. Faça-a com tranquilidade, mas controle o seu tempo.
4. Verifique se a prova é para o **PERFIL** para o qual concorre.
5. Somente após autorizado o início da prova, verifique se este Caderno de Questões está completo e em ordem. Folhear o Caderno de Questões antes do início da prova implica na eliminação do candidato.
6. Verifique, no **Cartão de Respostas**, se seu nome, número de inscrição, identidade e data de nascimento estão corretos. Caso contrário, comunique ao fiscal de sala.
7. O **Caderno de Questões** poderá ser utilizado para anotações, mas somente as respostas assinaladas no **Cartão de Respostas** serão objeto de correção.
8. Observe as seguintes recomendações relativas ao **Cartão de Respostas**:

- **.** não haverá substituição por erro do candidato;
- **.** não deixar de assinar no campo próprio;
- **.** não pode ser dobrado, amassado, rasurado, manchado ou conter qualquer registro fora dos locais destinados às respostas;
- **.** a maneira correta de marcação das respostas é cobrir, fortemente, com esferográfica de tinta azul ou preta, o espaço correspondente à letra a ser assinalada;
- **.** outras formas de marcação diferentes da que foi determinada acima implicarão a rejeição do **Cartão de Respostas**;

9. O fiscal não está autorizado a alterar quaisquer dessas instruções.
10. Você só poderá retirar-se da sala após 60 minutos do início da prova.
11. Quaisquer anotações só serão permitidas se feitas no caderno de questões.
12.Você poderá anotar suas respostas em área específica do Caderno de Questões, destacá-la e levar consigo.
13. Os três últimos candidatos deverão permanecer na sala até que o último candidato entregue o **Cartão de Respostas**.
14. Ao terminar a prova, entregue ao fiscal de sala, obrigatoriamente, o **Caderno de Questões** e o **Cartão de Respostas**.

Boa Prova!

Ao término de sua prova, anote aqui seu gabarito e destaque na linha pontilhada.

01	11	21	31	41	51
02	12	22	32	42	52
03	13	23	33	43	53
04	14	24	34	44	54
05	15	25	35	45	55
06	16	26	36	46	56
07	17	27	37	47	57
08	18	28	38	48	58
09	19	29	39	49	59
10	20	30	40	50	60