1 - Quadrix - 2025 - CRM-ES - Técnico de TI:
Processo de identificação do grau de importância dos ativos com base na confidencialidade, integridade e disponibilidade.
Esse processo ajuda a definir os níveis de proteção e priorizar recursos de segurança. Esse processo se denomina:

(X) classificação de ativos.
(B) ciclo de vida do ativo.
(C) inventário de ativos.
(D) controle de software.
(E) atribuição de responsáveis.

2 - Quadrix - 2025 - CRM-ES - Técnico de TI:
Assinale a opção que apresenta corretamente o conceito de vulnerabilidade.

(X) Falha, fraqueza ou brecha em sistemas, processos, pessoas ou controles que pode ser explorada para comprometer a confidencialidade, integridade ou disponibilidade das informações.
(B) Possibilidade de que um agente ou condição explore uma falha, fraqueza ou brecha e cause danos aos ativos de uma organização, como perda de dados, interrupção de serviços ou prejuízos financeiros.
(C) Qualquer evento, agente ou condição que possa causar dano a um sistema, a um ativo ou a uma organização e que representa o potencial de ocorrência de um incidente de segurança.
(D) Ocorrência identificada que compromete a confidencialidade, a integridade ou a disponibilidade das informações e envolve ações intencionais ou não intencionais.
(E) Ação deliberada realizada por um agente (humano ou automatizado) com o objetivo de explorar uma falha, fraqueza ou brecha, causar dano, obter acesso não autorizado ou interromper serviços.

3 - Quadrix - 2025 - CRM-ES - Agente Administrativo:
Um dos pilares da segurança das informações cadastrais preceitua que apenas pessoas autorizadas tenham acesso às informações, implicando a restrição do acesso aos sistemas informacionais e à implementação de políticas de controle de acesso.
Com base nessa informação, assinale a opção que apresenta a correta denominação desse pilar da segurança das informações.

(A) integridade
(B) disponibilidade
(X) confidencialidade
(D) autenticidade
(E) temporalidade

4 - Quadrix - 2025 - CRM-ES - Técnico Administrativo:
No que se refere a procedimentos básicos de segurança da informação, assinale a opção correta.

(A) Evitar atualizar o sistema, mantendo versões antigas, é recomendado para garantir compatibilidade e segurança.
(X) Manter sistemas operacionais e aplicativos sempre atualizados, bem como utilizar antivírus e firewall atualizados, são medidas preventivas de proteção.
(C) O uso de antivírus eliminou a necessidade de preocupações com senhas ou atualizações de software.
(D) É seguro clicar em qualquer link recebido por e-mail corporativo, desde computador possua firewall.
(E) Utilizar a mesma senha simples em todos os sistemas facilita o gerenciamento e reduz riscos de esquecimento, sendo uma prática aceitável de segurança.

5 - FEPESE - 2025 - CINCATARINA - Analista Técnico I:

O uso de fragmentadora de papel em órgãos públicos está relacionado principalmente à:

(A) Segurança da informação para impressão de documentos coloridos em grande escala.
(B) Segurança da informação para armazenamento de papéis para consulta futura.
(X) Segurança da informação, evitando acesso indevido a dados sigilosos.
(D) Segurança da informação para digitalização de documentos para sistemas eletrônicos.
(E) Segurança da informação para distribuição de cópias para vários setores.

6 - FEPESE - 2025 - CINCATARINA - Analista Técnico I:
Para proteger contas de e-mail e redes sociais, é essencial adotar boas práticas ao criar e usar senhas.
Assinale a alternativa que apresenta uma prática correta.

(A) Usar a mesma senha em todas as contas é mais seguro, pois facilita lembrar e gerenciar.
(B) Trocar senhas com frequência diminui a segurança, pois confunde os sistemas dos sites.
(C) Escolher senhas simples e comuns, como “123456” ou “senha”, é a forma mais segura e prática.
(D) Guardar todas as suas senhas em um arquivo de texto simples no computador é a melhor maneira de garantir que elas não sejam descobertas por criminosos.
(X) Criar senhas fortes, misturando letras maiúsculas e minúsculas, números e símbolos, e não as compartilhar com ninguém, aumenta a segurança das contas.

7 - AMEOSC - 2025 - Prefeitura de Iporã do Oeste - SC - Professor de

Informática - Edital nº 19:
Durante uma atividade pedagógica em laboratório de informática, um professor de informática percebeu que os computadores com Windows XP estavam apresentando lentidão e pop-ups constantes ao navegar na internet.
Para proteger os dados dos alunos e garantir o uso adequado das máquinas, ele decidiu adotar práticas de segurança digital.
Nesse contexto, é CORRETO afirmar que a ação adequada e tecnicamente correta a ser realizada em primeiro lugar é:

(A) Trocar o navegador padrão por outro de código aberto, evitando o uso de navegadores proprietários e fechado.
(B) Instalar atualizações do sistema operacional e ativar o firewall do Windows para evitar novas vulnerabilidades.
(X) Instalar e configurar um antivírus atualizado, realizar varredura completa e remover eventuais malwares identificados.
(D) Efetuar backup completo dos dados em mídia externa, formatar o computador e reinstalar todos os programas utilizados.

8 - FGV - 2025 - TCE-PE - Analista de Controle Externo - Tecnologia da Informação:
A confidencialidade, a autenticidade e a integridade constituem a base da segurança da informação.
Considerando esses princípios, estabeleça a correlação entre cada um deles e os protocolos ou algoritmos apresentados.
Princípios:

1. Confidencialidade
2. Autenticidade
3. Integridade Protocolos/Algoritmos:

( ) Kerberos
( ) 3DES (Triple Data Encryption Standard)

( ) SHA-1 (Secure Hash Algorithm 1)

Assinale a opção que indica a relação correta, na ordem apresentada.

(A) 1 – 2 – 3.
(B) 1 – 3 – 2.
(X) 2 – 1 – 3.
(D) 2 – 3 – 1.
(E) 3 – 1 – 2.

9 - VUNESP - 2025 - Câmara de Marília - SP - Auxiliar de Informática:
Um auxiliar de informática, que não tem acesso ao sistema de contabilidade, mas tem acesso ao banco de dados, recebeu um pedido de um analista da contabilidade para executar um SQL para alterar registros em um banco de dados desse sistema, alterando assim seus valores.
O auxiliar de informática sabe que isso não deve ser feito, porque viola um dos 3 pilares fundamentais da segurança da informação. Trata-se de:

(A) Confidencialidade.
(B) Disponibilidade.
(C) Monitoramento.
(X) Integridade.
(E) Acesso.

10 - FCC - 2025 - TRT - 2ª REGIÃO (SP) - Analista Judiciário - Área Administrativa - Contabilidade:
A servidora Ana trabalha na vara civil de um tribunal e frequentemente acessa sistemas judiciais, manipula documentos sigilosos e recebe e-mails com arquivos anexos.
Recentemente, percebeu lentidão no computador e janelas pop-up incomuns.
Para evitar riscos à integridade e confidencialidade das informações

tratadas, Ana decide adotar boas práticas de segurança digital com base na ação correta e segura no contexto da administração pública, que é:

(A) compartilhar senhas com colegas de equipe, desde que o objetivo seja facilitar o trabalho conjunto em processos urgentes.
(B) abrir os arquivos no e-mail institucional, pois isso garante que estão livres de vírus.
(C) desativar temporariamente o antivírus para permitir a abertura de anexos recebidos por e-mail institucional, confiando que se trata de documentos judiciais.
(X) manter o antivírus e o firewall ativados, evitar abrir anexos suspeitos e acionara equipe de TI ao notar comportamentos anormais no sistema.
(E) instalar softwares baixados de sites alternativos, desde que usados por colegas de trabalho a fim de agilizar o acesso aos documentos.