

SEGURANÇA DA INFORMAÇÃO VIII

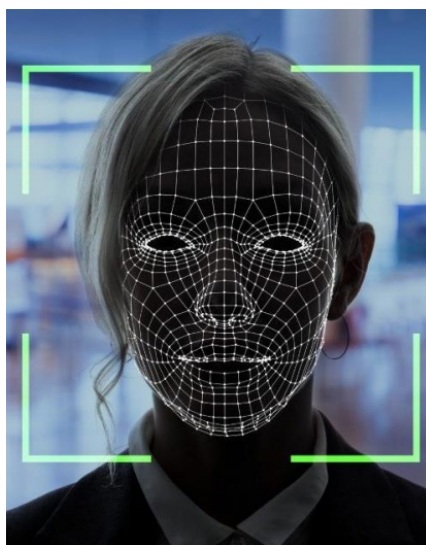
POLÍTICA DA MESA E DA TELA LIMPA

BIOMETRIA



Obs.: | o sistema não deve ser deixado logado na ausência do usuário. Também não devem ser deixados sobre a mesa objetos e papéis, principalmente se forem informações sigilosas.

BIOMETRIA



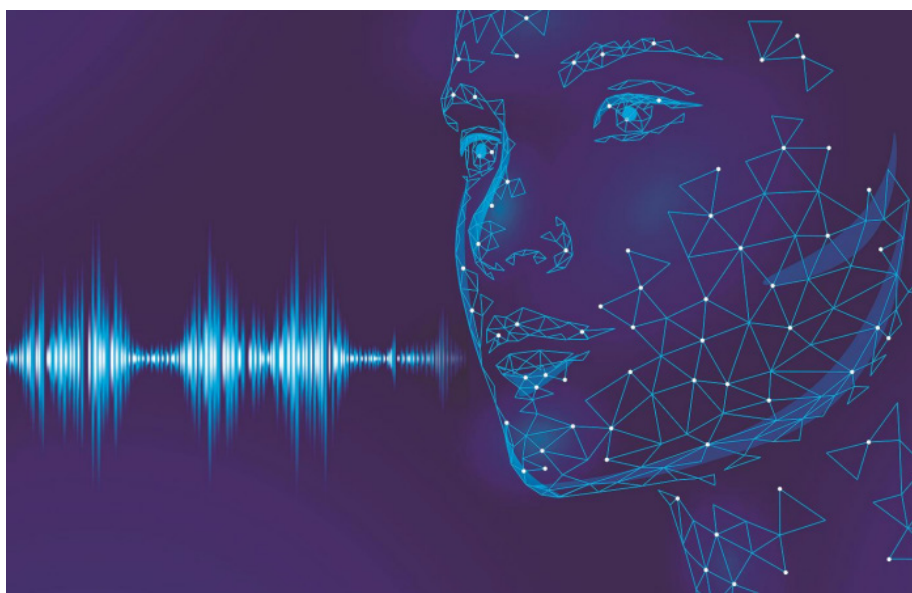
Obs.: | a leitura facial pode ser usada como método de validação.

BIOMETRIA



Obs.: | a leitura da digital também é uma forma de identificação do usuário.

BIOMETRIA



Obs.: | a voz também pode ser utilizada para identificação.

BIOMETRIA



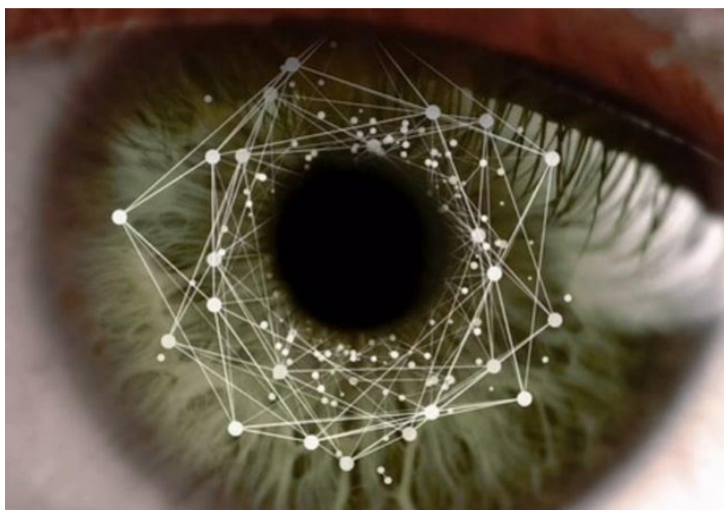
Obs.: | são avaliadas a letra, a posição e a pressão da escrita.

BIOMETRIA

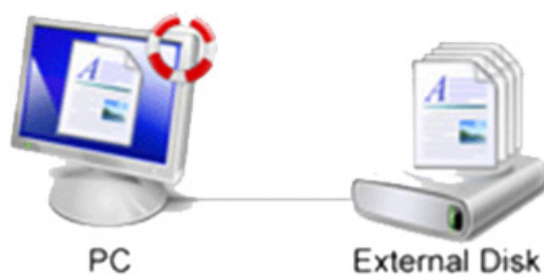


Obs.: | também pode ser utilizada a leitura da íris.

BIOMETRIA



BECAPIES



Obs.: | a cópia de segurança nunca deve ser feita no mesmo dispositivo onde estão os dados.

Da Classificação da Informação quanto ao Grau e Prazos de Sigilo (LEI N. 12.527)



Fonte: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

- I – ultrassecreta: 25 (vinte e cinco) anos;
- II – secreta: 15 (quinze) anos; e
- III – reservada: 5 (cinco) anos.

DIRETO DO CONCURSO

25. (2024/VUNESP/PMSP/SOLDADO PM DE 2ª CLASSE) Considere que a autoridade competente declarou como imprescindíveis à segurança da sociedade e do Estado e, portanto, classificou como ultrassecretas determinadas informações relativas à operação de inteligência relacionada à repressão de infração penal. Com base na Lei de Acesso à Informação (Lei no 12.527/11), pode-se dizer que o prazo máximo de restrição de acesso a essas informações, a contar de sua publicação, será de

- a. 100 anos.
- b. 5 anos.
- c. 15 anos.
- d. 50 anos.
- e. 25 anos.

26. (2023/QUADRIX/CRO/AGENTE FISCAL) Para adicionar maior proteção ao processo de autenticação de usuários, o uso de autenticação multifator (MFA) é indicado, porque adiciona duas ou mais camadas diferentes de verificação adicionais, como uso de aplicativos de autenticação, tokens físicos, reconhecimento facial e biometria.

27. (2024/CEBRASPE/ASSISTENTE DE TECNOLOGIA DA INFORMAÇÃO) No que se refere a mecanismos e técnicas de controle de acesso, julgue os seguintes itens. No contexto da segurança da informação, o controle de acesso restringe-se aos processos de autenticação.

28. (2022/LEGALLE CONCURSOS/BADESUL) Métodos de autenticação desempenham um papel crucial na segurança de sistemas e redes. Qual das seguintes alternativas descreve CORRETAMENTE o método de autenticação "token"?

- a. Forma comum de autenticação, em que os usuários fornecem um nome de usuário e uma senha. A segurança depende da complexidade da senha e da proteção contra adivinhação e ataques de força bruta.
- b. Usados para autenticar dispositivos, serviços ou indivíduos. Baseiam-se em criptografia de chave pública, onde um certificado é assinado por uma autoridade certificadora confiável. Garante a autenticidade e integridade das comunicações.
- c. Dispositivos físicos ou aplicativos que geram códigos temporários. Os usuários devem fornecer o código atual para autenticar. Comuns em autenticação de dois fatores (2FA) e autenticação de senha única (SSO).
- d. Utiliza características físicas exclusivas, como impressões digitais, reconhecimento facial, íris ou voz para verificar a identidade. Oferece um alto nível de segurança, pois é difícil de falsificar. Usado em sistemas de segurança avançados e autenticação biométrica de dispositivos móveis.



O token gerado dura alguns segundos.

29. (2024/ADM. TEC./TÉCNICO EM REDES DE COMPUTADORES III) Analise as informações a seguir:

- I – Considerando a Segurança da Informação na internet como conjunto de ações e estratégias para proteger sistemas, programas, equipamentos e redes contra invasões e ataques, não é preciso entrar em pânico nem autenticar senhas em duas etapas ou usar o gerenciador de senhas, por exemplo, já que as redes hoje contam com um forte sistema de proteção contra os ataques de hackers.
- II – Considerando a Segurança da Informação na internet como conjunto de ações e estratégias para proteger sistemas, programas, equipamentos e redes contra invasões e ataques, é importante fazer backup dos arquivos, usar backup em nuvem, sincronização com outro equipamento e HD externo ou Pendrive, além de fazer o backup no celular.
- III – Considerando a Segurança da Informação na internet como conjunto de ações e estratégias para proteger sistemas, programas, equipamentos e redes contra invasões e ataques, é aconselhável não clicar em tudo o que se receber, nem acionar link desconhecido, manter programas atualizados, verificar se as fontes dos sites são confiáveis, ler as avaliações dos sites em que se cadastrar e limitar as permissões ao navegar por determinados sites.

Marque a alternativa CORRETA:

- a. Todas as afirmativas estão corretas.
- b. Nenhuma afirmativa está correta.
- c. Apenas uma afirmativa está correta.
- d. Apenas duas afirmativas estão corretas.

30. (2024/ADM. TEC./TÉCNICO EM REDES DE COMPUTADORES) Analise as informações a seguir:

- I – É correto afirmar que já existem no mercado sistemas operacionais invioláveis, imunes a ataques hackers, protegidos por um potente firewall desenvolvido para bloquear o acesso não autorizado ao computador e garantir a segurança total da máquina.
- II – É correto afirmar que apenas os sites de má reputação ou de empresas de pequeno porte contém malware.

Marque a alternativa CORRETA:

- a. As duas afirmativas são verdadeiras.
- b. A afirmativa I é verdadeira, e II é falsa.
- c. A afirmativa II é verdadeira, e I é falsa.
- d. As duas afirmativas são falsas.

31. (2024/CEBRASPE/PCPE/ESCRIVÃO DE POLÍCIA) Assinale a opção que corresponde a uma prática recomendada em relação a backups.

- a. fazer backup apenas dos dados mais recentes
- b. usar um único método de backup
- c. ter múltiplas cópias de backup em locais diferentes
- d. armazenar todas as cópias de backup no mesmo local
- e. fazer backups uma vez por ano para economizar espaço

32. (2024/OBJETIVA CONCURSOS/PREFEITURA DE SÃO LUDGERO/FARMACÊUTICO) Um usuário está trabalhando em um ambiente onde a segurança das informações é de extrema importância. Durante o expediente, surge a necessidade de se ausentar temporariamente da sua mesa para participar de uma reunião rápida. Diante dessa situação, qual das seguintes medidas é a mais adequada e eficaz para o usuário prevenir o acesso não autorizado aos dados do seu computador?

- a. Fechar os aplicativos abertos.
- b. Bloquear o computador.
- c. Minimizar todas as janelas abertas.
- d. Desligar o monitor.



Política da tela limpa, sem login.

“Se você pensa que pode, ou que não pode, você está certo” – Henry Ford.

GABARITO

25. e

26. C

27. E

28. c

29. d

30. d

31. c

32. b

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jeferson Bogo Severino.

A presente gravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.
