-- CONHECIMENTOS ESPECÍFICOS --

A respeito de criptografia, julgue os itens seguintes.

101 Um dos exemplos de criptografia assimétrica é a de chave pública, baseada em funções matemáticas e não em funções de substituição e permutação.

102 A autenticidade de sistemas criptográficos garante que o conteúdo de uma mensagem não foi alterado.

103 Na criptografia simétrica, é possível obter o texto aberto a partir do texto cifrado quando se conhece qual é o algoritmo de encriptação, sem necessidade de se conhecer a chave secreta.

Julgue os próximos itens, com relação a vulnerabilidades e ataques.

104 Os ataques passivos costumam obter dados que estão sendo transmitidos, enquanto os ataques ativos buscam modificar ou criar um dado.

105 Instalações inadequadas e falta de controle de acesso são exemplos de vulnerabilidades organizacionais.

Com referência a políticas de segurança da informação, julgue os itens a seguir.

106 Cada informação deverá ter o seu próprio gestor, que será responsável por controlar suas autorizações de acesso e sua confidencialidade.

107 O objetivo da classificação da informação é definir o padrão de sigilo que será utilizado na organização e classificar cada informação considerando esse padrão.

Julgue os próximos itens, à luz do disposto na NBR ISO/IEC 27002:2022.

108 Deve-se permitir a identificação única de indivíduos e sistemas que acessem as informações de uma organização por meio da gestão de identidade; assim, são vedadas, expressamente e sem exceção, identidades atribuídas a várias pessoas, como, por exemplo, identidades compartilhadas, uma vez que é cogente responsabilizar a pessoa por ações realizadas com o emprego de uma identidade específica.

109 A segregação de funções e áreas de responsabilidade é importante em uma organização; entretanto, as funções de solicitação, aprovação e implementação de direitos de acesso não devem ser segregadas, devido ao princípio da unicidade de concessão de privilégios.

Julgue os seguintes itens, com base no que dispõe a NBR ISO/IEC 27001:2022.

110 A organização deve realizar avaliações de riscos da segurança da informação, bem como implementar o plano de tratamento de riscos da segurança da informação, retendo informação documentada dos resultados tanto das avaliações quanto do tratamento de riscos da segurança da informação.

111 No que se refere à conscientização, as pessoas que realizam trabalho sob o controle de uma organização devem estar cientes da política de segurança da informação desta, ainda que não seja necessário que conheçam as implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

Julgue os próximos itens, relativos a OWASP Top 10.

112 De acordo com o descrito para Insecure Design, um *design* inseguro não pode ser corrigido por uma implementação perfeita, sendo a falta de um perfil de risco empresarial inerente ao *software* que está sendo desenvolvido um dos fatores que contribuem para um *design* inseguro.

113 Quando explorado, o Broken Access Control permite a violação do princípio de menor privilégio, situação em que o acesso que deveria ser concedido para usuários específicos fica disponível para qualquer pessoa.

Julgue os itens a seguir, a respeito de *softwares* maliciosos.

114 *Worm* é um tipo de *software* malicioso que infecta uma estação de trabalho (*workstation*) em vez de infectar arquivos; ele não requer intervenção humana para se propagar e, diferentemente do vírus, não precisa se fixar em arquivo ou setor.

115 *Spyware* é um programa que se instala de maneira furtiva por meio de outro programa; ele monitora o usuário, capturando informações confidenciais, hábitos de consumo, senhas bancárias e informações de cartões de crédito.

116 Cavalo de troia (*trojan horse*) é um programa que promete uma ação ou funcionalidade, mas executa outra totalmente diferente; seu objetivo é enganar as pessoas, permitindo o acesso e o roubo de informações de seus computadores.

Acerca da segurança da informação, julgue os itens que se seguem.

117 A ocorrência, em uma empresa, da perda de comunicação com um sistema importante, seja pela queda de um servidor, seja pela aplicação crítica de negócio configura exemplo de perda de integridade.

118 A confidencialidade da informação garante que, em uma comunicação, a origem e o destino sejam realmente aquilo que alegam ser.

No que se refere à gestão de segurança da informação, julgue os itens subsecutivos.

119 Para se aplicar uma política de segurança da informação em uma organização, é suficiente que a alta direção da organização bem como os detentores dos demais cargos de liderança tenham conhecimento do teor da referida política e acompanhem a sua implantação.

120 O modelo de sistema de gestão de segurança da informação (SGSI) de uma organização é influenciado por fatores como necessidades e objetivos, requisitos de segurança, processos e estrutura organizacional.

Espaço livre