|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| 1 | O projeto do sistema deve conter um documento de especificação de segurança que descreve os objetivos de segurança do sistema. |  |  |
| 2 | O mecanismo de autenticação do usuário deve utilizar senhas com métrica mínima. |  |  |
| 3 | O mecanismo de autenticação do usuário deve exigir a troca periódica da senha. |  |  |
| 4 | O mecanismo de autenticação do usuário deve bloquear o acesso após número definido de tentativas de login com falha. |  |  |
| 5 | A senha deve ser verificada e autenticada em código situado fora do alcance do usuário. | S |  |
| 6 | A senha deve ser verificada por meio de mecanismo que impeça fraudes de repetição, interceptação ou quebra de integridade na comunicação entre o cliente e o servidor. |  |  |
| 7 | O sistema deve possuir um mecanismo de autorização formal para a criação de novos usuários no sistema. |  |  |
| 8 | Os novos usuários devem escolher sua senha sem a interferência do pessoal de apoio, no máximo recebendo uma senha inicial que precisa ser trocada. |  |  |
| 9 | A senha deve ser armazenada pelo sistema, cifrada de forma irreversível. |  |  |
| 10 | O sistema deve criar nova senha no caso do usuário ter perdido ou esquecido a sua. |  |  |
| 11 | Procedimentos formais para remoção de usuários do sistema, com eliminação imediata de direitos, devem ser adotados. |  |  |
| 12 | Antes do login ou uso do sistema, o usuário deve ter acesso a uma mensagem de limitação de responsabilidade. |  |  |
| 13 | Após o login do usuário, deve ser apresentada uma tela, com a data e hora do último login bem sucedido e se houve falhas de login desde então. |  |  |
| 14 | As mensagens de erro anteriores à autenticação do usuário devem indicar apenas informações indispensáveis. |  |  |
| 15 | O sistema de controle de acesso deve ser aplicado diretamente aos usuários e aos dados armazenados, indicando direitos para cada operação neste (leitura, escrita, criação, remoção, etc.), evitando-se o controle de acesso por funcionalidade. |  |  |
| 16 | O controle de acesso deve ser realizado por componente independente do resto do sistema, com interface bem definida. |  |  |
| 17 | O controle de acesso deve ser uniforme em todo o sistema, utilizando-se uma única rotina de verificação. |  |  |
| 18 | O sistema deve registrar os eventos significativos para a segurança |  |  |
| 19 | O sistema deve registrar falhas de login, indicando o número de tentativas. |  |  |
| 20 | O sistema deve registrar a criação e a remoção de usuários, bem como a designação e remoção de direitos do usuário. |  |  |
| 21 | O sistema deve registrar acessos e alterações em dados sensíveis mantidos pela aplicação. |  |  |
| 22 |  |  |  |
| 23 | A trilha de auditoria deve ser protegida contra remoção e alteração por parte de todos os usuários, exceto dos administradores de auditoria. |  |  |
| 24 | A trilha de auditoria deve sofrer inspeção periódica automatizada ou manual. |  |  |
| 25 |  |  |  |
| 26 | Os algoritmos de criptografia devem ser baseados em padrões reconhecidos do mercado. |  |  |
| 27 |  |  |  |
| 28 |  |  |  |
| 29 |  |  |  |
| 30 | Certificados digitais devem ser verificados contra as listas de revogação e contra a lista de CAs confiáveis. |  |  |
| 31 |  |  |  |
| 32 | O sistema deve possuir mecanismo de backup e restauração dos dados e do próprio sistema. |  |  |
|  |  |  |  |
| 34 | As entradas de dados devem ser verificadas contra valores esperados para campos. |  |  |
| 35 | Os dados recebidos de interfaces com outros sistemas devem ser validados conforme valores esperados e com o direito de acesso do outro sistema. |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 40 | Os ambientes de desenvolvimento, homologação e produção devem ser física e logicamente isolados. |  |  |
| 41 | O ambiente de desenvolvimento deve contar com um servidor de fontes com gerência de configuração. |  |  |
| 42 |  |  |  |
| 43 |  |  |  |
| 44 |  |  |  |
| 45 |  |  |  |
| 46 |  |  |  |
| 47 |  |  |  |