¿Cuál de los siguientes documentos de publicación especial del NIST proporciona una guía sobre cuestionarios y listas de verificación a través de los cuales se puede evaluar el cumplimiento de los sistemas con objetivos de control específicos?

- NIST SP 800-53A
- NIST SP 800-26
- NIST SP 800-53
- NIST SP 800-37
- NIST SP 800-59

Explicación: NIST SP 800-26 (Guía de autoevaluación de seguridad para sistemas de tecnología de la información) proporciona una guía sobre cuestionarios y listas de verificación a través de las cuales se pueden evaluar los sistemas cumplimiento de objetivos de control específicos

---

Conforme a FIPS 99. ¿Cuál de los siguientes niveles de impacto potencial muestra efectos adversos limitados en las operaciones de la organización, los activos de la organización o las personas? *

- Medio
- ajo
- BModerado
- Alto

¿Cuál de los siguientes es un estándar que establece requisitos básicos para evaluar la eficacia de los controles de seguridad informática integrados en un sistema informático?

- FITSAF
- FIPS
- SSAA
- TCSEC

¿Cuál de las siguientes normas ISO se titula "Tecnología de la información - Técnicas de seguridad - Gestión de seguridad de la información - Medición"?

- ISO 27005
- ISO 27006
- ISO 27004
- ISO 27003

¿Cuál de los siguientes documentos de publicación especial del NIST proporciona una guía sobre las pruebas de seguridad de la red?

- NIST SP 800-37
- NIST SP 800-42
- NIST SP 800-53A
- NIST SP 800-53
- NIST SP 800-60

¿Cuál de las siguientes normas ISO proporciona pautas para la acreditación de una organización que se ocupa de la certificación y el registro relacionados con el SGSI?

- ISO 27005
- ISO 27004
- ISO 27003
- ISO 27006

¿Cuál de los siguientes documentos del NIST proporciona una guía para identificar un sistema de información como un Sistema de Seguridad
Nacional?
a) NIST SP 800-37.
b) NIST SP 800-26.
c) NIST SP 800-53A,
d) NIST SP 800-59.

Explicación
NIST 800-59: Este documento es una guía para identificar un sistema de información como un Sistema de Seguridad Nacional

---

Trabaja como ingeniero de seguridad para BlueWell Inc. Desea utilizar algunas técnicas y procedimientos para verificar la efectividad de los controles de seguridad en el Sistema de Información Federal. ¿Cuál de los siguientes documentos del NIST lo guiará?
a) NIST SP 800-37.
b) NIST SP 800-26.
c) NIST SP800-53A.
d) NIST SP 800-59.

Explicación
NIST 800-53A. Este documento consta de técnicas y procedimientos para verificar la efectividad de los controles de seguridad en el Sistema de Información Federal.

¿Cuál de las siguientes normas ISO se titula "Tecnología de la información - Técnicas de seguridad - Gestión de seguridad de la información - Medición"?
a) ISO 27003.
b) ISO 27005.
c) ISO 27004.
d) ISO 27006.

Explicación
ISO 27004 es un estándar de seguridad de la información desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Se titula "Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Medición". La norma ISO 27004 proporciona directrices sobre especificaciones y el uso de técnicas de medición para la evaluación de la eficacia de un sistema y controles de gestión de seguridad de la información implementados.

¿Cuáles de los siguientes son obligatorios para su uso en sistemas federales?
a) Serie NIST SP 800
b) FIPS
c) NISTIR.
d) Boletines de seguridad del DIT

Explicación
Los estándares federales de procesamiento de información (FIPS) son requisitos obligatorios para los sistemas federales.

El Estándar Federal de Procesamiento de Información (FIPS) que prescribe pautas para la autenticación biométrica es:

- FIPS 201
- FIPS 186.
- FIPS 197.
- FIPS 140.

Comentarios
La Verificación de identidad personal (PIV) de empleados y contratistas federales se publica como FIPS 201 y prescribe algunas pautas para la autenticación biométrica

---

¿Cuál de los siguientes es el Estándar federal de procesamiento de información (FIPS) actual que especifica un algoritmo criptográfico aprobado para garantizar la confidencialidad de los datos electrónicos?

- Estándar de firma digital (FIPS 186).
- Requisitos de seguridad para módulos criptográficos (FIPS 140).
- Verificación de identidad personal (PIV) de empleados y contratistas federales (FIPS 201).
- Estándar de cifrado avanzado (FIPS 197).

Comentarios

El Estándar de cifrado avanzado (AES) especifica un algoritmo criptográfico aprobado por FIPS que se puede utilizar para proteger datos electrónicos. El algoritmo AES es un cifrado de bloque simétrico que puede cifrar y descifrar información. El cifrado convierte los datos a una forma ininteligible llamada texto cifrado; descifrar el texto cifrado convierte los datos a su forma original, denominada texto sin formato. El algoritmo AES es capaz de utilizar claves criptográficas de 128, 192 y 256 bits para cifrar y descifrar datos en bloques de 128 bits

---

¿Cuál de los siguientes es un estándar de seguridad multifacético que se utiliza para regular las organizaciones que recopilan, procesan y / o almacenan datos de titulares de tarjetas como parte de sus operaciones comerciales?

- NIST SP 800-64.
- FIPS 201.
- ISO / IEC 15408.
- PCI DSS

Comentarios

El PCI DSS es un estándar de seguridad multifacético que incluye requisitos para la gestión de seguridad, políticas, procedimientos, arquitectura de red, diseño de software y otras medidas de protección críticas. Este estándar integral está destinado a ayudar a las organizaciones a proteger de manera proactiva los datos de las cuentas de los clientes.