



## Ejercicios de repaso y autoevaluación

- 1. Cuando se define una política de control de accesos hay que tener en cuenta una serie de requerimientos definidos en la normativa ISO 27002:2013. Indique a qué requerimiento pertenecen las siguientes medidas de seguridad:**

Gestion de acceso de los usuarios

- a. Gestión de las claves secretas de los usuarios mediante un procedimiento formal.

control de acceso a la red

- b. Segregación de los grupos de servicios de información, usuarios y sistemas de información en redes distintas.

Responsabilidad user

- c. Adopción de una política de escritorio y pantalla limpios.

- d. Establecimiento de procesos que cierren las sesiones en los sistemas operativos de los usuarios que superen un período de inactividad indefinido.

control de acceso al so para evitar accesos no autorizados

- 2. Complete la siguiente oración:**

En la política de control de acceso deben establecerse las reglas de control de acceso y los derechos para cada Usuario o grupo de usuarios, los controles deben ser tanto lógicos como físicos y considerarse conjuntamente

- 3. El procedimiento formal para el registro de usuarios debe incluir una serie de principios. ¿Cuál de las siguientes frases no se corresponde con estos principios?**

- a. Comprobar que el usuario dispone de la autorización para el uso del sistema de información.

- b. Facilitar a los usuarios un documento escrito donde estén reflejados sus derechos de acceso.



- c. Promover el desarrollo y la utilización de aquellas aplicaciones que eviten la necesidad de utilizar privilegios.

- d. Mantener un registro formal de todas las personas autorizadas para utilizar el sistema de información.

- 4. Los directivos y gerentes de una organización deben encargarse de la revisión periódica de los derechos de acceso de los usuarios. Esta revisión debe realizarse mediante un procedimiento formal. Indique qué debe incluir, como mínimo, este procedimiento.**

que deben revisarse periódicamente

deben reasignarse con el cambio de puesto del trabajador

las autorizaciones y privilegios especiales deben revisarse con mayor frecuencia y hay que llevar un registro de los cambios realizados al menos en las cuentas con privilegios especiales

**5. ¿Qué Norma ISO recoge los requerimientos para definir una correcta política de acceso a los sistemas de información de una organización?**

- a. ISO 27001:2003
- b. ISO 27002:2003 27002:2013
- c. ISO 27003:2003
- d. ISO 27004:2004

**6. Identifique los siguientes enunciados con cada tipo de medidas que debe adoptar e implantar el responsable de un fichero:**

- |              |  |
|--------------|--|
| Técnico      | a. Medidas cuyos objetivos están encaminados a mantener la integridad, confidencialidad y disponibilidad de la información cuando esta contiene datos de carácter personal. Estas medidas están clasificadas en función del nivel de seguridad de sus datos: básico, medio y alto. |
| Organizativa | b. Medidas cuyos objetivos están encaminados al establecimiento de procedimientos, normas, reglas y estándares de seguridad para proteger los datos personales en el momento de su tratamiento.  |

**7. Según la LOPDGDD, ¿qué nombre recibe el responsable de los datos dentro de una organización?**

- a. Responsable de ficheros.
- b. Responsable del tratamiento de ficheros.
- c. Responsable del tratamiento de datos.
- d. Responsable de datos.

**8. Comente qué acciones podrá realizar un usuario con los permisos siguientes:**

- |                     |  |
|---------------------|--|
| leer y ejecutar     | a. El usuario podrá ejecutar aquellas aplicaciones que no influyan en los datos de la organización y también podrá visualizar los archivos, aunque no realizará ninguna modificación en ellos. |
| control total       | b. El usuario ya está autorizado para hacer cualquier tipo de operación sobre los archivos en los que se les ha asignado este permiso, desde su creación, modificación hasta su eliminación.   |
| lista de contenidos | c. El usuario podrá abrir las carpetas para visualizar los archivos que hay en ella, pero no podrá acceder a ellos.  |
| solo lectura        | d. El usuario con estos permisos solo podrá leer y visualizar los ficheros. No podrá ejecutar ninguna aplicación.  |

**9. Rellene las medidas de seguridad que falten en el listado.**

Conservacion de los datos un minimo de 2 años

El responsable de tratamiento de datos debe establecer un mecanismo de identificación de los usuarios que tratan de acceder al sistema

asi como tambien debe controlar los mecanismos de registro de datos

En accesos autorizado almacenar la informacion e identificar el registro accedido

---

## MEDIDAS DE SEGURIDAD

---

Almacenamiento de la identificación, fecha y hora del acceso, fichero accedido, tipo de acceso y acceso autorizado/denegado en cada acceso.

---

Control de acceso físico limitado al personal autorizado en el documento de seguridad.

---

establecer mecanismos para evitar el acceso de usuarios con derechos distintos a los autorizados

---

Acceso autorizado solo a los datos necesarios.

---

la concesion y modificacion del acceso autorizado solo puede realizarlo el personal autorizado en el doc. de seguridad  
limitacion de intentos reiterados de autentificacion

---

Revisión de la información de control y elaboración de informes: una vez al mes por el responsable de seguridad.

---

relacion de usuarios que contenga el acceso autorizado de cada uno

---

### 10. Relacione las siguientes definiciones con los protocolos mencionados a continuación:

- a. Es una base de datos jerárquica en la que se almacena información sobre los nombres de dominio en las redes. Su utilización más frecuente está relacionada con la asignación de nombres de dominio a las direcciones IP.
- b. Es un protocolo que asigna de modo automático las direcciones IP.
- c. Es un protocolo de autenticación de usuarios que permite que dos equipos situados en una red de baja seguridad se puedan identificar mutuamente de un modo seguro.
- d. Se trata de un protocolo que permite el acceso a un servicio de directorio ordenado y distribuido cuya función principal es permitir la búsqueda de información en un entorno de red. En numerosas ocasiones, es considerado como una base de datos sobre la que se puede realizar una serie de consultas para localizar los datos deseados.

B DHCP.

c Kerberos.

d LDAP.

a DNS.

**11. ¿Qué es un directorio activo?**

es un servicio de directorio que tiene las características de una red para configurar accesos

---

---


**12. Indique a qué hacen referencia las siguientes claves utilizadas con frecuencia en DLAP:**

- a. u. unit o department
- b. sn. surname
- c. cn. common name
- d. givenname. apodo

**13. Complete la siguiente oración:**

La gestión de identidades y autorizaciones (IAM) es un conjunto de sistemas y procesos encargados de gestionar y controlar la identidad de las personas que acceden a los recursos del sistema y todo aquello que puede hacer cada usuario con estos recursos, cumpliendo en todo momento con las políticas definidas por la organización.

**14. ¿Cuál de los siguientes aspectos no está incluido en un perfil de identidad?**

- a. Información personal del usuario.
- b. Credenciales de autenticación.
-  c. Identificación común.
- d. Permisos de acceso y roles asignados al usuario.

**15. Relacione las siguientes definiciones con cada tipo de herramienta SSO:**

- a. Protocolo que externaliza la autenticación de los usuarios a través del servidor Kerberos.
- b. Herramienta mediante la cual se evitan autenticaciones redundantes para identificar a los usuarios en aplicaciones web.
- c. Herramienta que compila la identidad en una dirección url, que puede ser verificada posteriormente por cualquier aplicación o servidor para conocer la identidad y los privilegios del usuario que pretende acceder a ellos.
- d. Herramienta que utiliza una autenticación primaria para completar automáticamente las aplicaciones secundarias con el mismo usuario y contraseña.

b Identidad federada.

c OpenID.

a Kerberos.

d Enterprise Single Sign-On (E-SSO) o Legacy Single Sign-On.