TEST DE EVALUACIÓN

CONTRASEÑAS

Y medidas complementarias

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE

www.incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TEST

Selecciona para cada pregunta la respuesta correcta.

1. La robustez es una característica fundamental de las contraseñas basada principalmente en:

a) La longitud de esta y el tipo de caracteres utilizados.

b) Lo difícil que sea de recordar.

c) El número de letras mayúsculas utilizadas.

d) Todas las anteriores.

2. Una contraseña robusta debe estar compuesta por:

a) Un mínimo de 8 caracteres y que contenga números y letras.

b) Un mínimo de 8 caracteres y que contenga números, letras mayúsculas, minúsculas y símbolos.

c) Un mínimo de 8 caracteres y que contenga letras mayúsculas, minúsculas y símbolos.

d) Un mínimo de 16 caracteres y que sean números.

3. Los generadores de contraseñas son la mejor forma de obtener contraseñas robustas. Indica su principal inconveniente:

a) Si son generadas utilizando un equipo antiguo o con pocos recursos computacionales estas serán menos robustas.

b) Suelen añadir más cantidad de números que de otros caracteres por lo que algunas veces no son suficientemente robustas.

c) No son generadas aleatoriamente y predecirlas es una tarea trivial para cualquier ciberdelincuente.

d) La complejidad para ser recordadas debido a su aleatoriedad.

4. Los gestores de contraseñas son:

a) Funciones que incorporan las aplicaciones web para verificar si una contraseña es correcta o no.

b) Herramientas que permiten almacenar múltiples contraseñas de diferentes servicios.

c) Herramientas que utilizan los ciberdelincuentes para «adivinar» las contraseñas de sus víctimas.

d) Ninguna de las anteriores.

5. Indica la respuesta correcta:

a) Las contraseñas deben ser secretas, es decir, no se deben compartir con nadie.

b) Las contraseñas son el único método para acceder a cualquier servicio o dispositivo.

c) Las contraseñas pueden ser compartidas cuando el servicio al que dan acceso no es crítico para la empresa.

d) Las contraseñas deben ser modificadas al menos una vez cada tres meses.

6. Uno de los errores más habituales cuando se utilizan contraseñas es:

a) Utilizar una contraseña débil.

b) Utilizar la misma contraseña para múltiples servicios.

c) Escribirla en un post-it o similar a la vista de cualquiera.

d) Todas las anteriores.

7. Indica cuál de las siguientes contraseñas es la más robusta:

a) 123165498789

b) Carmen8899

c) 0cT4€Dro1990?

d) C4m1@n

8. El doble factor de autenticación es:

a) Un mecanismo que añade una capa extra de seguridad a los servicios que requieren de usuario y contraseña para su uso por medio una nueva clave que, generalmente, es de un solo uso.

b) Un mecanismo que permite a dos usuarios acceder a un mismo servicio por medio de una única contraseña.

c) Un mecanismo utilizado en exclusiva por las redes sociales para verificar la identidad del usuario.

d) Una estrategia que utilizan algunos servicios en Internet que permite su acceso por medio de dos contraseñas distintas.

9. Cuando se utiliza un gestor de contraseñas, su punto más crítico es:

a) Ninguno, ya que es un software diseñado para no tener ningún punto débil.

b) El dispositivo que lo esté ejecutando, siempre y cuando se encuentre libre de malware y completamente actualizado.

c) La robustez de la contraseña maestra que da acceso al servicio.

d) El máximo de contraseñas que permite almacenar.

10. ¿Cuál de las siguientes afirmaciones es falsa?

a) Las contraseñas, como el nombre de nuestra mascota seguido del año de nacimiento de nuestro hijo, son las más recomendables porque son fáciles de recordar.

b) La reutilización de las contraseñas es uno de los errores más comunes.

c) Se ha de utilizar, si es posible, doble factor de autenticación para los servicios que se utilizan en Internet.

d) La contraseña debe ser intransferible.

SOLUCIONES

PREGUNTA	RESPUESTA
1	A
2	B
3	D
4	B
5	A
6	D
7	C
8	A
9	C
10	A

TEST DE EVALUACIÓN

CONTRASEÑAS

Y medidas complementarias

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE
www.incibe.es
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD