TEST DE EVALUACIÓN

EL PUESTO DE TRABAJO

Medidas de protección I

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. El puesto de trabajo, desde el punto de vista de la ciberseguridad para la empresa:

a) Es clave, ya que de este dependerá en gran medida que la compañía no sufra un incidente que puede afectar a su continuidad.

b) Está expuesto a múltiples riesgos como perdida de confidencialidad, infecciones por malware o información en formato físico accesible por terceras partes.

c) Debe ser protegido por el propio empleado siguiendo las políticas y recomendaciones indicadas por los responsables de la empresa.

d) Todas las anteriores.

2. Indica la respuesta correcta:

a) La documentación en formato físico puede contener información confidencial, que debe estar siempre bajo custodia del empleado y ser guardada en un lugar seguro al terminar la jornada laboral.

b) Las contraseñas de acceso a los servicios corporativos pueden apuntarse en un *post- it* para que sean más fáciles de recordar.

c) No es necesario que el puesto de trabajo esté limpio y ordenado.

d) Las memorias USB y discos duros externos pueden estar siempre conectados al dispositivo incluso cuando termina la jornada laboral.

3. Indica la respuesta correcta sobre el bloqueo de sesión:

a) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia del mismo, a excepción de tablets y smartphones.

b) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia del mismo, excepto si se encuentra dentro de la empresa, ya que es un lugar seguro.

c) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia del mismo.

d) No es necesario habilitar un bloqueo de sesión.

4. El atajo de teclado para bloquear un dispositivo con sistema operativo Windows es:

a) Win + L

b) Win + B

c) Win + X

d) Win + Fin

5. Mantener el software actualizado es:

a) Algo que no es realmente importante, ya que mientras funcione de forma correcta es suficiente.

b) Una necesidad, pero solo para el sistema operativo. No es necesario que las diferentes herramientas que incorpora estén actualizadas, ya que la seguridad del dispositivo no depende de estas.

c) Algo de lo que no es necesario estar preocupado ya que todo se actualiza de forma automática sin necesidad de interacción por parte del usuario.

d) Una necesidad. Todo el software, incluido el sistema operativo, debe estar actualizado a la última versión disponible en cualquier dispositivo.

6. Cuando el software de un equipo esta desactualizado, se corre el riesgo de:

a) Contar con medidas de seguridad que pueden haber quedado obsoletas.

b) Todas las respuestas son ciertas.

c) Que un ciberdelincuente utilice alguna vulnerabilidad para tomar el control del dispositivo.

d) No poder utilizar las últimas funcionalidades ofrecidas por el fabricante.

7. El antivirus es:

a) Una herramienta innecesaria y que consume muchos recursos.

b) Una herramienta que protege contra el software malicioso solo en los ordenadores.

c) Una herramienta indispensable en cualquier dispositivo, incluidos los dispositivos móviles.

d) Todas las anteriores.

8. Un cortafuegos o *firewall* es:

a) Una herramienta innecesaria en los dispositivos si se cuenta con antivirus.

b) Una herramienta que controla las comunicaciones que se producen con otros dispositivos o Internet reduciendo el riesgo de que se produzca un incidente de seguridad.

c) Una herramienta que protege el dispositivo contra software malicioso.

d) Ninguna de las anteriores.

9. Indica la respuesta correcta sobre el antivirus y el *firewall*:

a) No pueden estar habilitados de manera simultánea ya que una herramienta interferiría con la otra de manera muy negativa para el dispositivo.

b) No es necesario que estén actualizados.

c) Deben estar habilitados ambos a la vez y actualizados, ya que aumentan considerablemente la seguridad del equipo.

d) No son herramientas de seguridad necesarias ya que aumentan el consumo de recursos y la protección que ofrecen frente al malware es mínima.

10. ¿Cuáles son buenas prácticas para la protección del puesto de trabajo?

a) Disponer de una política de mesas limpias, difundirla y hacerla cumplir.

b) Mantener todo el software actualizado.

c) Instalar, activar y mantener actualizados los antivirus y cortafuegos.

d) Todas las anteriores, además de bloquear la sesión cuando no estemos frente a nuestros dispositivos.

SOLUCIONES

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

TEST DE EVALUACIÓN

EL PUESTO DE TRABAJO

Medidas de protección I

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