Ciberseguridad

para Estudiantes de Escuela Intermedia

Libro de actividades y preguntas de prueba

¡Pon a prueba tu conocimiento sobre ciberseguridad!

División de Asuntos del Consumidor de Nueva Jersey

800-242-5846 ■ www.NJConsumerAffairs.gov

ESTADO DE NUEVA JERSEY
OFICINA DEL FISCAL GENERAL
DIVISIÓN DE ASUNTOS DEL CONSUMIDOR

Estimado/a estudiante,

La capacidad de conectarte al Internet es un privilegio, y la protección de tu seguridad en línea es tu responsabilidad. Aunque probablemente eres un/a usuario/a del Internet con experiencia en computadoras, y cuentas con un gran conocimiento y las herramientas para expresar tu creatividad, debes darte cuenta que el Internet también presenta ciertos riesgos. Todas las aplicaciones móviles y en línea, tales como sitios de juegos, de redes sociales y de entretenimiento, suponen diferentes problemas de seguridad.

Este folleto te proveerá recomendaciones básicas que puedes usar mientras navegas por el Internet. Te animamos a respaldar el compromiso y ayudar a proteger tu seguridad, la de tus amigos y parientes a la hora de usar el Internet.

Atentamente,

Tus amigos en la División de Asuntos del Consumidor de Nueva Jersey

Probablemente te conectas al Internet con mucha frecuencia,

… y por medio de teléfonos celulares, computadoras portátiles (*laptops*), y aparatos para jugar, te mantienes conectado/a al mundo externo. Los usas para mantenerte en contacto con tus amistades y tus parientes. Los usas para hacer la tarea, y para tomar fotos. Los usas para enterarte si ganó tu equipo favorito. Los usas incluso para hacer compras. No hay duda que conectarse al Internet tiene sus ventajas. Pero también existen peligros ocultos. A continuación te proveemos ciertas herramientas para que las utilices, para que te protejas, y para que protejas y resguardes tu información personal cuando te conectas al Internet:

★ **No** te comuniques con personas desconocidas en línea y nunca aceptes reunirte en persona con alguien que no conozcas.

★ **Infórmale a uno de tus padres o a otro adulto en todo momento** si alguien que no conoces se comunica contigo por medio de correo electrónico, o por mensajes de texto, o por una aplicación.

★ **No compartas tu información personal por ningún motivo,** a menos de que uno de tus padres o tu tutor te diga que está bien. Tu información personal incluye tu nombre, tu dirección, tu edad, tu número de teléfono, tu fecha de cumpleaños, tu dirección de correo electrónico, la escuela a la que asistes, y otros datos sobre tí.

Antes de navegar por el Internet, asegúrate de preguntarte lo siguiente:

- ¿Diría yo en persona las cosas que publico en las redes sociales?
- ¿Son hirientes o groseras o perjudiciales, de alguna manera, mis actividades en línea?
- ¿Me gustaría que alguien me tratara así?
- ¿Me gustaría que uno de mis padres, o tutores, o abuelos, o maestros, u otro adulto vea lo que publico por Internet?
- ¿Cuáles son las consecuencias por lo que publico?
- ¿Qué clase de historia digital estoy creando?
- ¿Qué clase de imagen digital estoy creando sobre quien soy?
- ¿De qué manera afectarán mis actividades digitales mis amistades o mi futuro?
- ¿Conozco la persona con quien me comunico cuando me conecto al Internet?

6 SUGERENCIAS PARA ESTUDIANTES

1. Jamás compartas tu contraseña con nadie, excepto con tus padres o tu tutor.

2. Si sientes que alguien te está acosando o amenazando, cuéntale a un padre, a un tutor o a un maestro.

3. Publicar algo por Internet es lo mismo que escribir usando un marcadador permanente. No se puede borrar.

4. NO existe la anonimidad en el Internet. Tu computadora tiene una dirección en el mundo cibernético, al igual que tu casa tiene una dirección en el mundo real.

5 **Mantén privada tu información personal. Jamás compartas ninguna información personal por Internet.**

6 **Respeta a otras personas. Si no te gustaría que digan cosas sobre tí, no digas cosas sobre otras personas.**

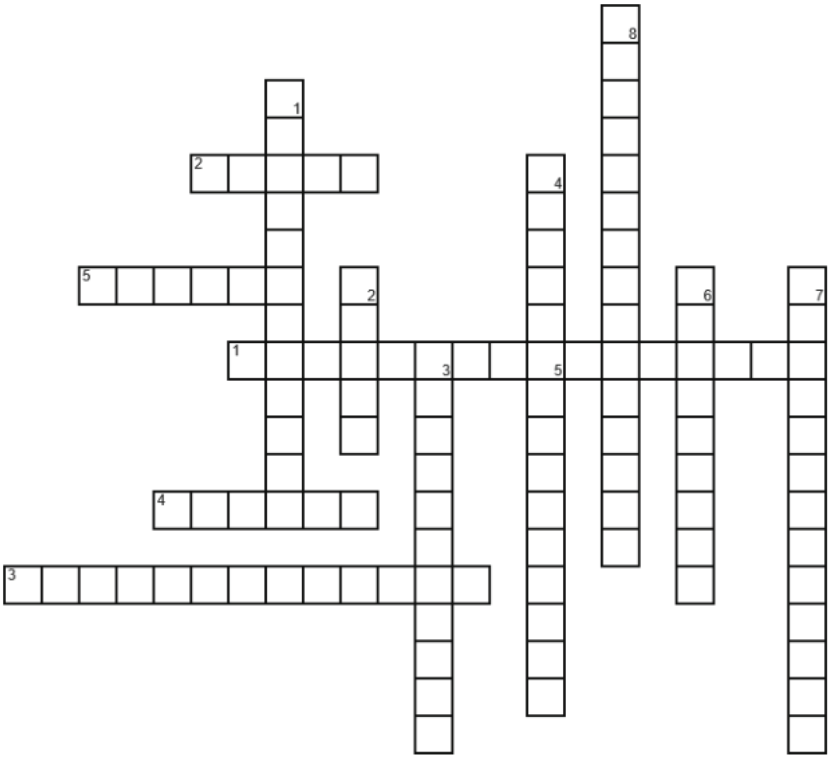
Pón a prueba TU conocimiento sobre ciberseguridad y juega las actividades que aparecen en las siguientes páginas.

Sopa de letras sobre *ciberseguridad*

g l d w z s u r i v i t n a o d w e
d e s c a r g a r o d a t u p m o c
p a g i n a i n i c i a l s e c m f
b o v p r o g r a m a m a l i g n o
l i o c i t e n r e b i c n o t a m
w r u d a t o s p e r s o n a l e s
b a s a l a d e c h a r l a s v t p
b u s c a r a m i s t a d e s r f r
a s o a p l i c a c i o n g f o k i
n u g e a i p s e a m a r g o r p v
e e e e i n a l a m b r i c a s a a
s d u o t x e t e d e j a s n e m c
a e f g c o r r e o b a s u r a j i
r r a m e d i o s s o c i a l e s d
t b t r o d a r o l p x e d k r r a
n m r i n t e r n e t w i t t e r d
o o o e u g o l b d o m i n i o t d
c n c e n l i n e a c o o k i e z n

Datos personales	Medios sociales	Matón cibernético	Buscar amistades
Cortafuegos	Nombre de usuario	Página inicial	Inalámbrica
Contraseña	Internet	Antivirus	Computadora
Programa maligno	Twitter	Virus	Privacidad
Descargar	Mensaje de texto	Sala de charlas	Blogueo
Programa espía	Explorador	En línea	Cookie
Dominio	Correo electrónico	Correo basura	Aplicación

Crucigrama de *ciberseguridad*



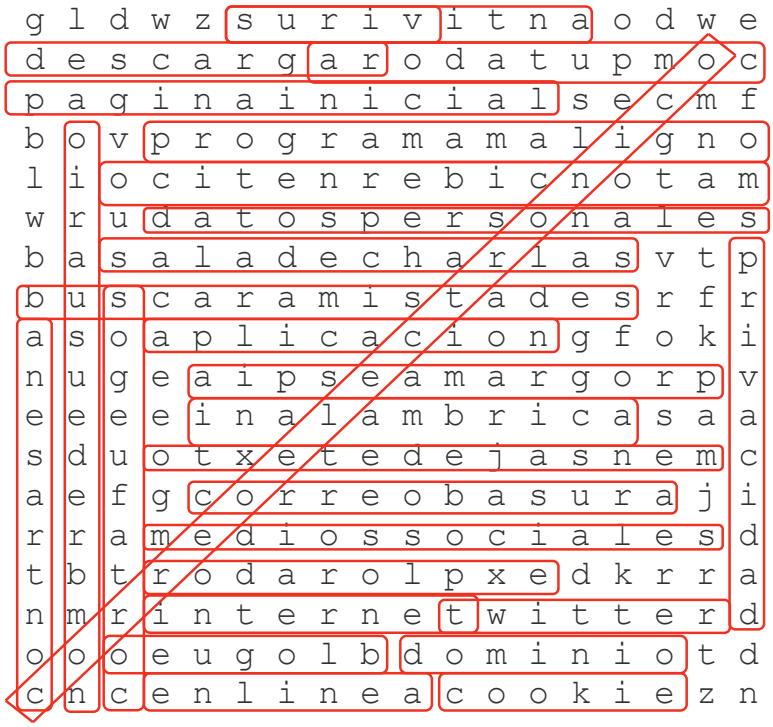
Horizontales	Verticales
1. Una persona que utiliza el Internet para acosar a otras personas (por ejemplo, al enviar mensajes rudos por redes sociales). 2. Una clase de programa malicioso que se autoreproduce (clona) a fin de propagarse a otras computadoras. Por lo general, los clones se desplazan por una red de computadoras e infectan a múltiples computadoras. 3. Una clase de software malicioso (o *malware*) que causa que aparezcan ventanas éxtra de publicidad en tu pantalla. A menudo, estas ventanas contienen enlaces que dirigen al usuario a sitios con un contenido inapropiado o con ventanas pop-up. 4. Alguien que trata de utilizar codificación para alterar o modificar un sitio web en existencia, creando programas malignos y piratear a otras personas/computadoras/compañías. 5. Un software que puede hacer cosas perjudiciales a tu computadora, tales como robar datos, borrar archivos, o apoderarse de tu computadora.	1. Correos o comentarios electrónicos no deseados en los que se venden o dicen cosas que no te interesan. 2. Una imágen o ícono digital que expresa algo (por lo general, una emoción). 3. Un sistema que impide el acceso no autorizado a una computadora por medio de una red, tal como el Internet. 4. No se trata de una galleta. Es un archivo pequeño enviado a un explorador web que lleva un registro de información como tu ubicación, tus preferencias al hacer compras, y otras decisiones que tomas. 5. Un programa que utilizas para explorar el Internet (por ejemplo, Internet Explorer o Safari). 6. Un programa que instalas en tu computadora o teléfono para protegerlo contra virus o programas maliciosos que podrían robar tu información o dañar tu aparato. 7. Una clase de software que te espía, y roba tus datos y contraseñas. 8. Hacerse pasar por otra persona en Internet por medio de robar información personal, tal como los detalles de una cuenta bancaria.

Conecta las palabras de *ciberseguridad*

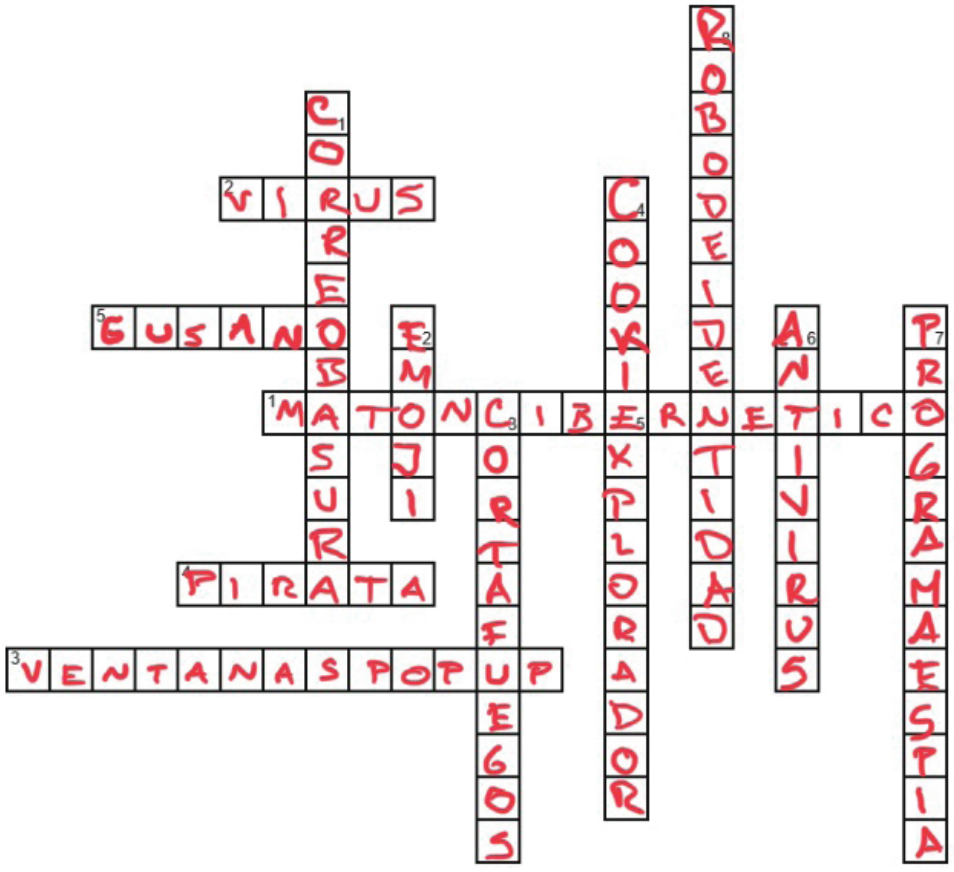
1 _____ Contraseña	A. Reglas o costumbres para interactuar de manera cortés en línea con otras personas (tales como no escribir un mensaje totalmente en mayúsculas, lo cual equivale a gritar).
2. _____ Correo basura (*Spam*)	B. Un código secreto que creas para proteger tu información personal, y para evitar que otras personas tengan acceso a tus archivos de computadora.
3. _____ Huella digital	C. Un delito relacionado a obtener la información personal de otra persona (nombres, tarjeta de crédito, número de seguro social, números de una cuenta bancaria), usualmente con el fin de robar dinero.
4. _____ Nombre de usuario	D. Correo con un contenido similar a desechos, desperdicios, chatarra, etc.
5. _____ Netiqueta	E. Programas perjudiciales que le dicen a tu computadora que haga cosas destructivas, las cuales pueden dañar tu computadora, así como sus archivos y documentos, o que permita que alguien, en efecto, te observe.
6. _____ Virus	F. Una ventana de explorador que se abre al azar cuando ingresas a una página web.
7. _____ Robo de identidad	G. Un término que creas para tener acceso a información protegida.
8. _____ Ventanas pop-up	H. Un registro electrónico guardado por las computadoras en el que se documentan todas las visitas a sitios web y mensajes por correo electrónico, los cuales aun pueden existir incluso después de eliminar el historial del explorador y borrar los mensajes de correo electrónico.
9. _____ Ciberestafa	I. El intento de engañar a las personas para que visiten sitios web maliciosos por medio de enviar correos electrónicos, u otros mensajes que fingen venir de bancos o de tiendas en línea.

Guía de respuestas: 1 (B) 2(D) 3(H) 4 (G) 5(A) 6(E) 7(C) 8(F) y 9(I)

Solución a la Sopa de letras sobre *ciberseguridad*



Solución al Crucigrama de *ciberseguridad*



Normas para una contraseña inteligente y segura

- **Jamás compartas tu contraseña con nadie, excepto con tus padres y/o tus tutores.**

Sin importar qué tan fuerte sea la tentación, jamás compartas tus contraseñas con tus amistades, sin importar lo estrecha que sea la relación contigo. Es posible que, sin quererlo, tu amistad comparta tu contraseña con otras personas. Puede que una ex-amistad decida abusar de la contraseña y, a fin de causarte mal, compartirla deliberadamente con otras personas.

- Utiliza contraseñas inteligentes.

- Asegúrate de utilizar ocho carácteres, como mínimo.

- Utiliza una combinación de letras mayúsculas y minúsculas, al igual que números y símbolos tales como # $!

- Al emplear palabras comunes, utiliza letras alternativas o carácteres para que te permita darle más complejidad a la contraseña, y para que sea más fácil de recordarla.

Algunos ejemplos son:

S = $

E = 3

a= @

¡ = !

O = 0

B = 8

- Utiliza contraseñas que las personas no puedan adivinar fácilmente.

- No utilices contraseñas basadas en información personal que un pirata, o *hacker*, pueda adivinar con facilidad o a la cual pueda tener fácil acceso. Por ejemplo, las contraseñas JAMÁS deberían contener información personal, tal como tus nombres o apellidos, tu fecha de nacimiento, el nombre y apellido de soltera de tu madre, la dirección residencial, el nombre o dirección de tu escuela, número de una tarjeta de crédito, o un número de teléfono.

- No utilices palabras que se pueden encontrar en el diccionario.

- En la medida posible, crea una "frase de contraseña." Enlaza varias palabras en una frase que te sea fácil recordar, y utiliza la letra inicial de cada palabra para crear una contraseña. Por ejemplo, la frase "Comencé el 5to grado en Washington Middle School en 2016" se convertiría en la siguiente contraseña: "Ce5geWMSe2016."

- No utilices solamente una contraseña.

Utiliza siempre una contraseña diferente para los distintos sitios que visites. Si utilizas solamente una contraseña y alguien obtiene acceso a esta contraseña, podrían utilizarla para ingresar a las cuentas que tengas en otros sitios.

Pon a prueba tu conocimiento sobre contraseñas

Lee cada frase y decide si es cierta o falsa.

1. Deberías cambiar tus contraseñas con frecuencia.	_____ Cierto _____ Falso
2. Robert01112 es una contraseña segura.	_____ Cierto _____ Falso
3. Deberías utilizar la misma contraseña en todos los sitios que visites, así como en todos tus aparatos.	_____ Cierto _____ Falso
4. "SusanB" es una contraseña segura.	_____ Cierto _____ Falso
5. Deberías utilizar contraseñas en todo momento, para que puedas bloquear el acceso a tus pantallas en todos tus aparatos móviles y computadoras.	_____ Cierto _____ Falso
6. «$3gURID@D¡» es una contraseña segura.	_____ Cierto _____ Falso
7. Deberías compartir tus contraseñas únicamente con tus padres.	_____ Cierto _____ Falso
8. «GonzalezLuis»» es una contraseña segura.	_____ Cierto _____ Falso
9. Jamás compartas tus contraseñas con tus amistades.	_____ Cierto _____ Falso
10. "MePBJs!" es una contraseña segura.	_____ Cierto _____ Falso

Guía de respuestas: 1-Cierto, 2-Falso, 3-Falso, 4-Falso, 5-Cierto, 6-Cierto, 7-Cierto, 8-Falso, 9-Cierto, 10-Cierto

Compromiso de Ciberseguridad

ME COMPROMETO A:

1. Reflexionar antes de publicar

Prometo no publicar información o imágenes que podrían ponerme en riesgo, o avergonzarme, o causar daños a mi futuro, tales como:

- los números del teléfono celular o de casa
- la dirección de casa
- información personal, tal como mi nombre, mi dirección, mi escuela, mi cumpleaños, o mi dirección de correo electrónico
- fotografías y videos inapropiados

2. Respetar a otras personas en línea

No voy a:

- publicar nada que sea grosero, ofensivo, o amenazante
- enviar o remitir imágenes e información que pudieran avergonzar, lastimar, o acosar a otra persona
- apoderarme de la información personal de otra persona y usarla para causar daño a su reputación

3. Asegurarme de que conozco a mis amistades cibernéticas

Acuerdo en que:

- nunca me comunicaré en línea con personas extrañas
- nunca me reuniré en persona con un desconocido
- le contaré a mis padres, a mi tutor o a mi maestro si una persona desconocida me está siguiendo por el Internet

4. Protegerme a mí mismo en línea

Si alguien me hace sentir incomodo o si alguien es descortés u ofensivo:

- se lo contaré a mis padres, a un tutor, o a otro adulto de confianza
- reportaré el incidente al sitio web o a la plataforma, a la compañía del teléfono celular, y a la policía
- guardaré las pruebas
- no le responderé

Firma / Fecha

Ciberseguridad

para Estudiantes de Escuela Intermedia

NJConsumerAffairs.gov/CyberSafe

División de Asuntos del Consumidor de Nueva Jersey

800-242-5846 ■ www.NJConsumerAffairs.gov