

CIBER SEGURO

Una guía perruna sobre seguridad en Internet



Renee Tarun & Susan Burg

FORTINET

CIBER SEGURO

CIBER SEGURO: una guía perruna
sobre seguridad en Internet



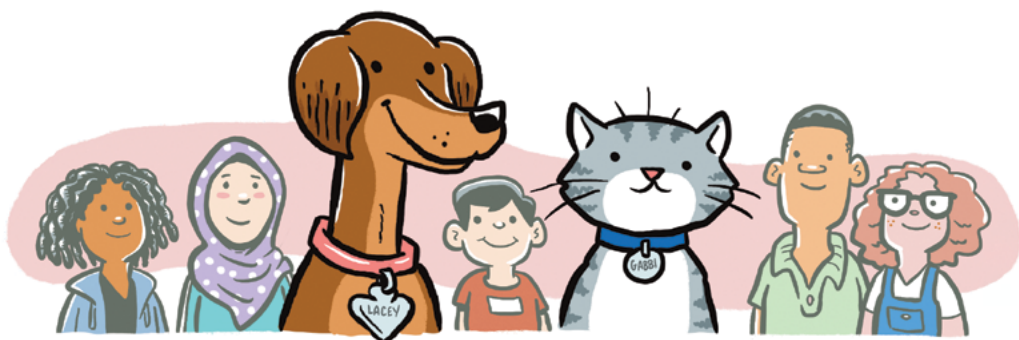
Por Renee Tarun y Susan Burg

Ilustraciones: Terry LaBan

FORTINET.

ÍNDICE

¿Qué es Internet?.....	4
¿Qué puedes hacer en Internet?.....	5
¿Por qué Ciberseguridad?.....	6
Contraseñas: Cierra la puerta.....	8
Actualizaciones y software antivirus.....	10
No hagas clic: Cuídate del phishing.....	11
No hables con extraños.....	12
Cómo mantenerte seguro.....	13
Publicar en las redes.....	14
Ser un buen compañero.....	15
Glosario.....	16
Recuerda P.A.T.A. para mantenerte seguro.....	17
Guía para padres.....	18



Para mis hijos, Ryan y Becca - Los amo
y deseo que siempre estén seguros!

Para Brett - gracias por ser siempre mi luz.

-Renee Tarun

A todos mis estudiantes que ahora son de todas las edades:

Manténganse seguros en línea y tomen buenas decisiones.

Quiero que algún día digan, "La sra. Burg, me enseñó
mucho...

igual que el perro y el gato del libro Ciber Seguro".

-Susan Burg

Copyright © 2020 by Fortinet

Todos los derechos reservados. Esta publicación en parte o en su totalidad, no puede ser reproducida, distribuida o transmitida en cualquier forma o por cualquier medio, incluyendo fotocopias, grabaciones u otros métodos electrónicos o mecánicos, sin el permiso previo por escrito de Fortinet, excepto en el caso de breves citas incorporadas en revisiones críticas y otros ciertos otros no comerciales permitidos por la ley de derechos de autor. Para solicitudes de permiso, escriba al autor, dirigido a "Attention: Permissions" a cybersafe@fortinet.com.

Fortinet
899 Kifer Rd.
Sunnyvale, CA 94086

Primera edición

Traducción: Heidi Wolf y Paula Fiszman.

Sobre las autoras

Renee Tarun es una mamá con más de 20 años de experiencia en ciberseguridad. Es la subdirectora de Seguridad de la Información (CISO) en Fortinet; antes de eso, trabajó en la Agencia de Seguridad Nacional (NSA) de Estados Unidos.

Susan Burg es una maestra certificada por la Junta Nacional con 24 años de experiencia en docencia. Le encantan los niños y le encanta escribir; actualmente, está trabajando en una serie de novelas juveniles sobre una niña llamada Gracie.

Renee y Susan son buenas amigas que comparten la pasión por mantener a los niños seguros en línea. Los personajes del libro se inspiraron en sus mascotas, Lacey y Gabbi, que trajeron tanta alegría y felicidad a sus familias. Han dejado sus huellas en nuestros corazones para siempre.

Agradecimientos

Queremos agradecer a Fortinet por apoyar este libro y por su profundo compromiso con la seguridad cibernética tanto para niños como para adultos.





¿QUÉ ES INTERNET?



Internet conecta computadoras en todo el mundo. Los niños y los adultos lo usan todos los días.



¡Muchas cosas sorprendentes están conectadas a Internet!

Refrigeradores



Juguetes



Luces



Tímbrs



Autos



Televisores



OTRAS FORMAS DE CONECTARSE A INTERNET



¿QUÉ PUEDES HACER EN INTERNET?

Ver videos



Hablar con amigos y familiares



Buscar y explorar



Escuchar música



Aprender casi cualquier cosa



Jugar juegos



Descubrir qué está pasando



Pero ¿por qué tengo que preocuparme por la seguridad? Todo es divertido.

A eso voy...



POR QUÉ CIBERSEGURIDAD



PELIGROS EN EL CIBERESPACIO

Mundo real
Pescar un pez



En línea
Carnada con cosas gratis



Mundo real
Enfermarse



En línea
Virus de computadora



Mundo real
Robo de dinero y objetos



En línea
Robo de dinero y datos

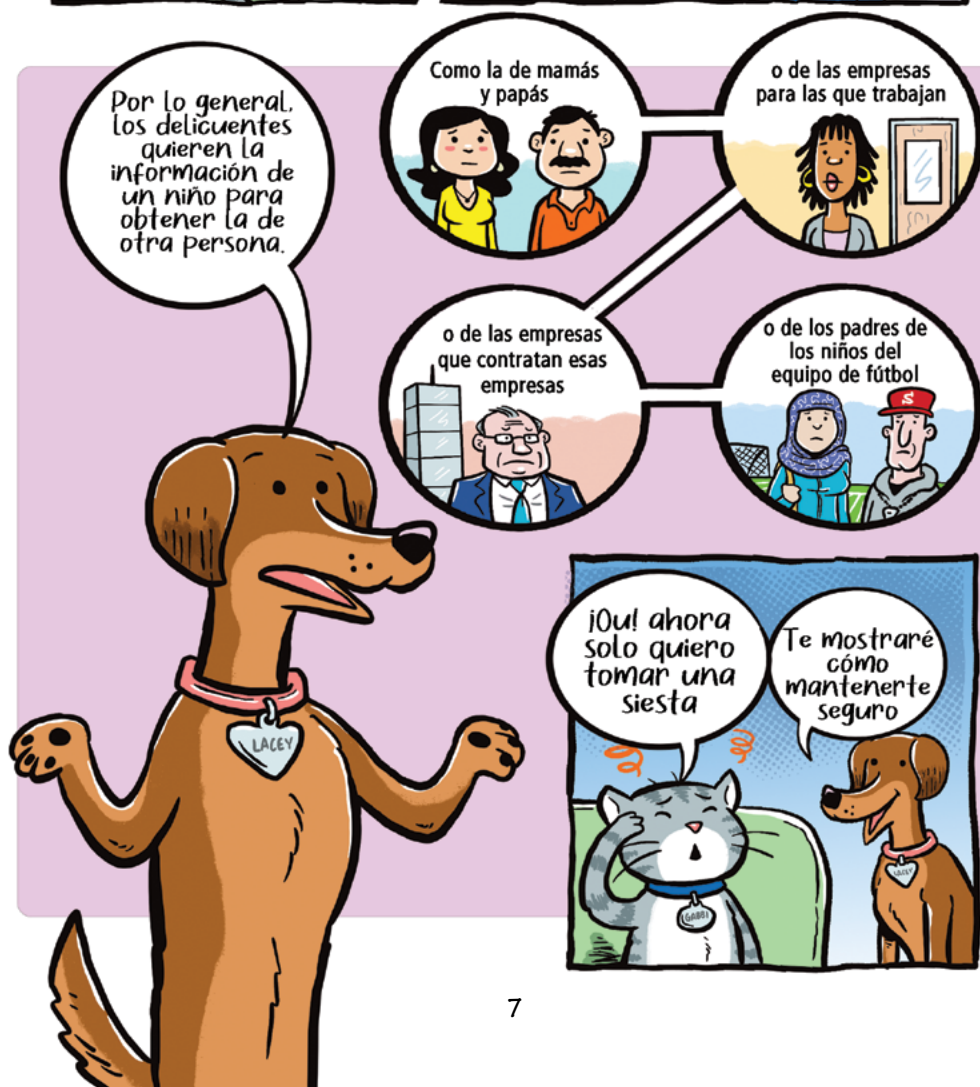


Mundo real
Escuchar la conversación de otros



En línea
Espiar desde un Wi-Fi público





CONTRASEÑA CIERRA LA PUERTA





¿Sabías? la mayoría de los delincuentes utilizan contraseñas robadas o débiles para entrar en la cuenta de las personas

REGLAS PARA Contraseñas

☒ **ELIGE UNA CONTRASEÑA QUE SOLO TÚ CONOZCAS**
No use sus datos personales: fecha de cumpleaños, dirección, edad o número de teléfono.



☒ **QUE SEA DIFÍCIL DE ADIVINAR**
Usa letras mayúsculas y minúsculas, números y caracteres especiales como \$, # y %



☒ **MANTÉNLO EN SECRETO**



☒ **SI ALGO NUEVO VIENE CON UNA CONTRASEÑA, CÁMBIALA**



☒ **NO USES ESTAS CONTRASEÑAS COMUNES (Y MALAS)**

Secreto Fútbol Contraseña
1234567 ABCDE

TAMBIÉN ES MALO

Usar letras como números
P3RR0

¡Y no uses a tus celebridades, películas, juegos o personajes de dibujos animados favoritos!



Las mejores contraseñas son más largas y complicadas



MALA
perropeludo82

MEJOR
%P3RR0PeLUdo#82!

Usa siempre un código de acceso para bloquear tabletas y teléfonos



ACTUALIZACIONES Y SOFTWARE ANTIVIRUS



TEN CUIDADO DE:



NO HAGAS CLIC EN:



CUÍDATE DEL PHISHING

Abre solo correos electrónicos de personas que conoces.



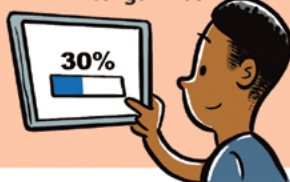
Si algo se ve mal, pregúntale a la persona si en verdad lo envió.



No hagas clic en los enlaces.



Antes de abrir un archivo adjunto (como una imagen o un video), revisa que no tenga virus.



¿Sabías? phishing significa engañar a alguien para que haga clic en un enlace que hace algo malo.

NO HABLES CON EXTRAÑOS



Algunos extraños se hacen pasar por niños. Los extraños en línea pueden ser tan peligrosos como los extraños de la vida real.

CUIDADO CON LOS EXTRAÑOS

PREGÚNTATE

¿Conozco a esta persona?



CÓMO MANTENERTE SEGURO

Habla solo con personas que conoces en la vida real.



No compartas información personal en línea.



No confíes en extraños ni escuches a extraños.



Nunca aceptes reunirse con extraños en persona.



No sigas a un extraño de una aplicación a otra.



Si un extraño dice que no le digas a nadie, deberías definitivamente contárselo a alguien.



Si algo te parece extraño en línea, habla con un adulto de confianza



PUBLICAR EN LAS REDES



Protege toda tu información. Nunca des tu nombre, número de teléfono, correo electrónico, contraseña, domicilio, escuela o tu foto sin el permiso de tus padres.



Consulta a un adulto de confianza antes de publicar algo en línea.



SER UN BUEN COMPAÑERO



EL CIBERACOSO ES UN GRAN PROBLEMA

Es lo mismo que acosar en persona, pero el acosador se esconde detrás de un teclado.



Algunas personas dicen cosas en línea que no te dirían a la cara.



¡El ciberacoso hierde!



LO QUE SÍ PUEDEN HACER LOS NIÑOS

No respondas a publicaciones maliciosas o hirientes.



Habla con tus papás o maestros si ves ciberacoso.



Se amable y respetuoso con todos.





Actualizaciones

Las últimas funciones y correcciones para computadoras y dispositivos. A menudo incluyen soluciones a problemas de seguridad.

Antivirus

Software que protege computadoras y dispositivos contra virus y malware.

Ciberacosar

Ser malo con otra persona en Internet.

Ciberespacio

Otro término para Internet.

Ciberseguridad

Prácticas para mantenerse seguro en línea.

Clic

Para seleccionar algo en una pantalla, ya sea mediante el tacto, el mouse, el teclado o comandos de voz.

Código de acceso

Un código o patrón que desbloquea un dispositivo como un teléfono o una tableta.

Correo electrónico masivo

Correo electrónico no deseado enviado a muchas personas. Puede contener virus o estafas. También conocido como spam.

Datos personales

Información personal como números de teléfono, cumpleaños, direcciones, etc.

En línea

Conectarse a Internet.

Extraño

Cualquier persona que no conoces.

Información personal

Incluye todos los detalles sobre ti, como edad, nombre, dirección, el color de tu cabello, fecha de nacimiento, escuela, grado, equipos deportivos, ciudad donde naciste y más.

Internet

Una red mundial de computadoras interconectadas.

Malware

Abreviatura de software malicioso (malo). El malware incluye adware (publicidad no deseada), virus, spyware (software espía), gusanos (malware que se multiplica solo) y mucho más.

Password (contraseña)

Una secuencia secreta de letras, números y caracteres que te permiten acceder a software o sitios web.

Phishing

Un intento de recopilar información personal mediante el envío de un correo electrónico engañoso o la creación de un sitio web engañoso.

Publicar

Poner cualquier cosa en línea (palabras, imágenes, videos).

Wi-Fi público

Wi-Fi disponible en lugares públicos que no está encriptado (codificado para privacidad)

Virus

Un virus informático es un programa que está diseñado para propagarse a otras computadoras, haciéndolas vulnerables a los ataques.

Recuerda P. A. T. A. para estar seguro.

P

ROTEGE

tu información personal y no publiques nada sin el permiso de tus padres.



A

TENCIÓN

ante cualquier invitación que sea de extraños, nunca te reúnas con ellos en persona.



T

AMBIÉN

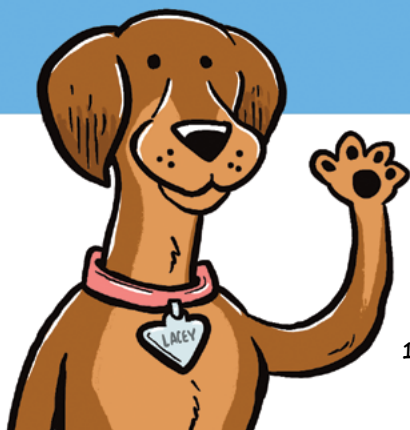
si ves algo triste, incómodo o confuso, habla con un adulto de confianza.



A

CTÚA

de manera positiva y no respondas a publicaciones malas o hirientes.



GUÍA

Hable con sus hijos

Considere establecer límites en torno a lo siguiente:

- Defina cuánto tiempo se les permite a los niños estar en línea
- Dígalos qué sitios pueden visitar.
- Especifique el software que pueden usar
- Permita actividades o tareas que sean apropiadas para su edad en función de su conocimiento y madurez.

Dé prioridad a la privacidad

Publicar información personal o fotos en Internet puede ser peligroso, ya que puede ser utilizado por personas que quieran causar daño.

- Una vez compartidas, las fotos y la información personal pueden tener efectos inquietantes más adelante.
- Es difícil eliminar algo una vez que está en el dominio público.
- Verifique la configuración de privacidad en los sitios de redes sociales para evitar que extraños accedan a información personal. Es posible que estos ajustes no se establezcan correctamente de forma predeterminada.

Explique las cuatro cosas que NO deben hacer:

- No dar su nombre, número de teléfono, dirección de correo electrónico, contraseña, dirección, escuela o fotografía sin permiso.
- No responder a publicaciones maliciosas o hirientes.
- No abrir correos electrónicos ni archivos adjuntos de personas que no conocen.
- No aceptar reunirse con nadie que “conozcan” en línea.

Si ven algo, digan algo

- Hable con sus hijos sobre los peligros de Internet para que reconozcan comportamientos o actividades sospechosas.
- Hágalos saber a sus hijos que, si ven algo en un sitio web, en un correo electrónico o en un chat que no les parece correcto o los hace sentir incómodos, pueden acudir a usted con sus preguntas e inquietudes.

PARA LOS PADRES

Mantenga todo actualizado

- Los padres deben instalar todas las actualizaciones en los dispositivos y aplicaciones de su computadora.
- Los padres deben instalar y ejecutar software antivirus.

Manténgase informado y atento

- Sepa lo que hace su hijo en la computadora, incluidos los sitios web que visita.
- Si usan correo electrónico, mensajería instantánea o salas de chat, asegúrese de tener una idea de con quién se están comunicando en línea.
- Asegúrese de que su hijo conozca realmente a las personas con las que está hablando en línea.

Coloque las computadoras en espacios abiertos

- Si su computadora está en un área común, puede monitorear fácilmente la actividad de la computadora.
- Si los niños se dan cuenta de que puede ver la pantalla, les ayuda a evitar que hagan cosas que no debieran.
- La visibilidad le da la oportunidad de intervenir si nota un comportamiento que podría tener consecuencias negativas.

Pregúntele a su proveedor de Internet sobre los controles parentales

Algunos proveedores de Internet ofrecen servicios (a veces gratuitos) diseñados específicamente para proteger a los niños en línea al restringir el acceso a sitios web o búsquedas de funciones de comunicación como correo electrónico, chat y mensajería instantánea, por edad, contenido, tiempo y otras categorías. Comuníquese con su proveedor para averiguar qué ofrece.

Aproveche más controles parentales

Algunos navegadores web le permiten restringir o permitir solo ciertos sitios web, y puede proteger estas configuraciones con una contraseña. Si bien ninguna tecnología es infalible, considere usar aplicaciones que ofrezcan protección adicional al monitorear, filtrar y restringir el acceso al contenido peligroso.

Todo el mundo dice que hay que tener cuidado en línea. Pero ¿a qué se refieren?

Lacey es un perro cibernético muy inteligente que protege a los niños enseñándoles cómo mantenerse seguros en línea. Únete a Lacey y a su amigo Gabbi en una divertida aventura cibernética y aprende cómo actuar y cómo mantenerte seguro en línea.

