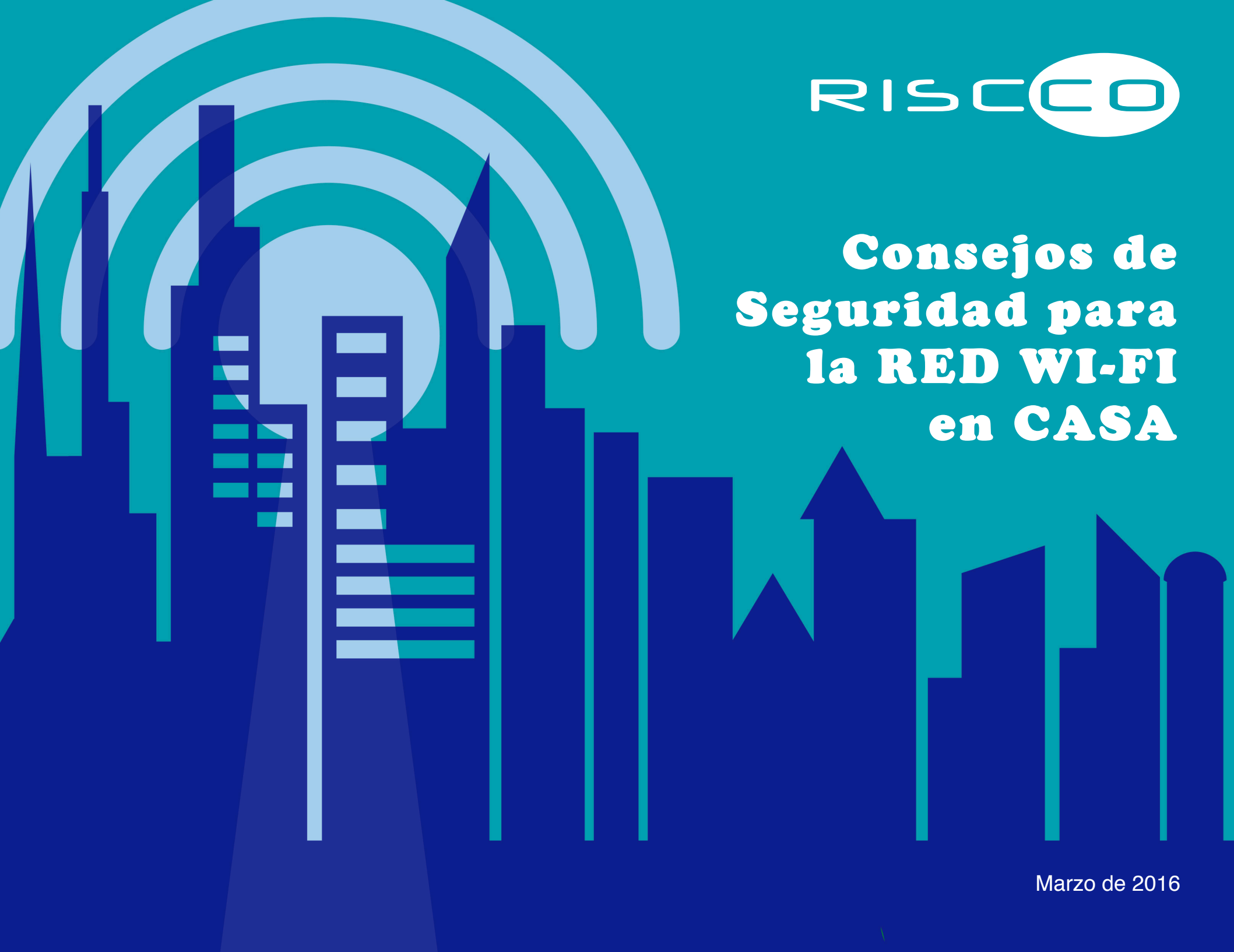
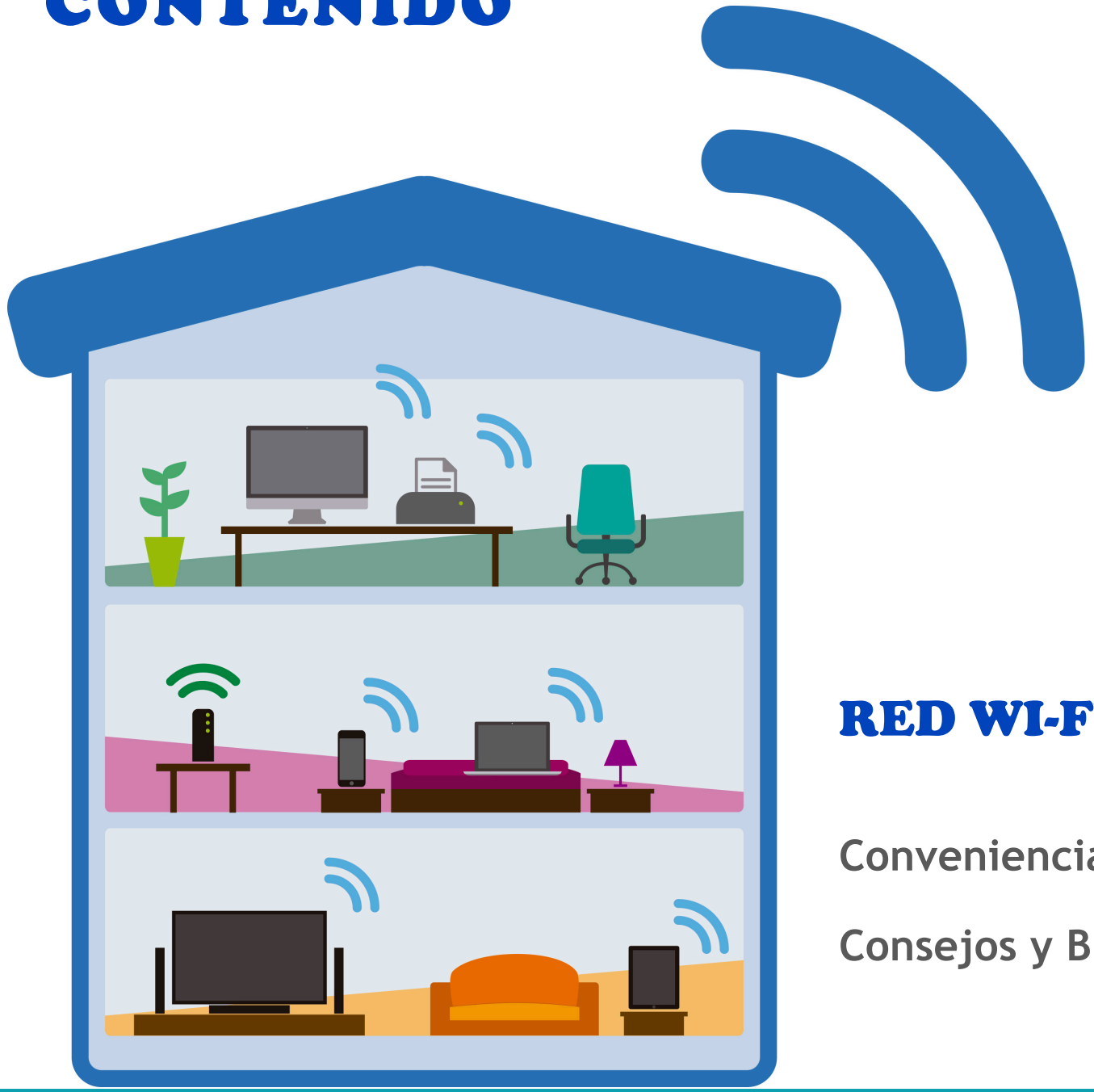


RISCO

Consejos de Seguridad para la RED WI-FI en CASA

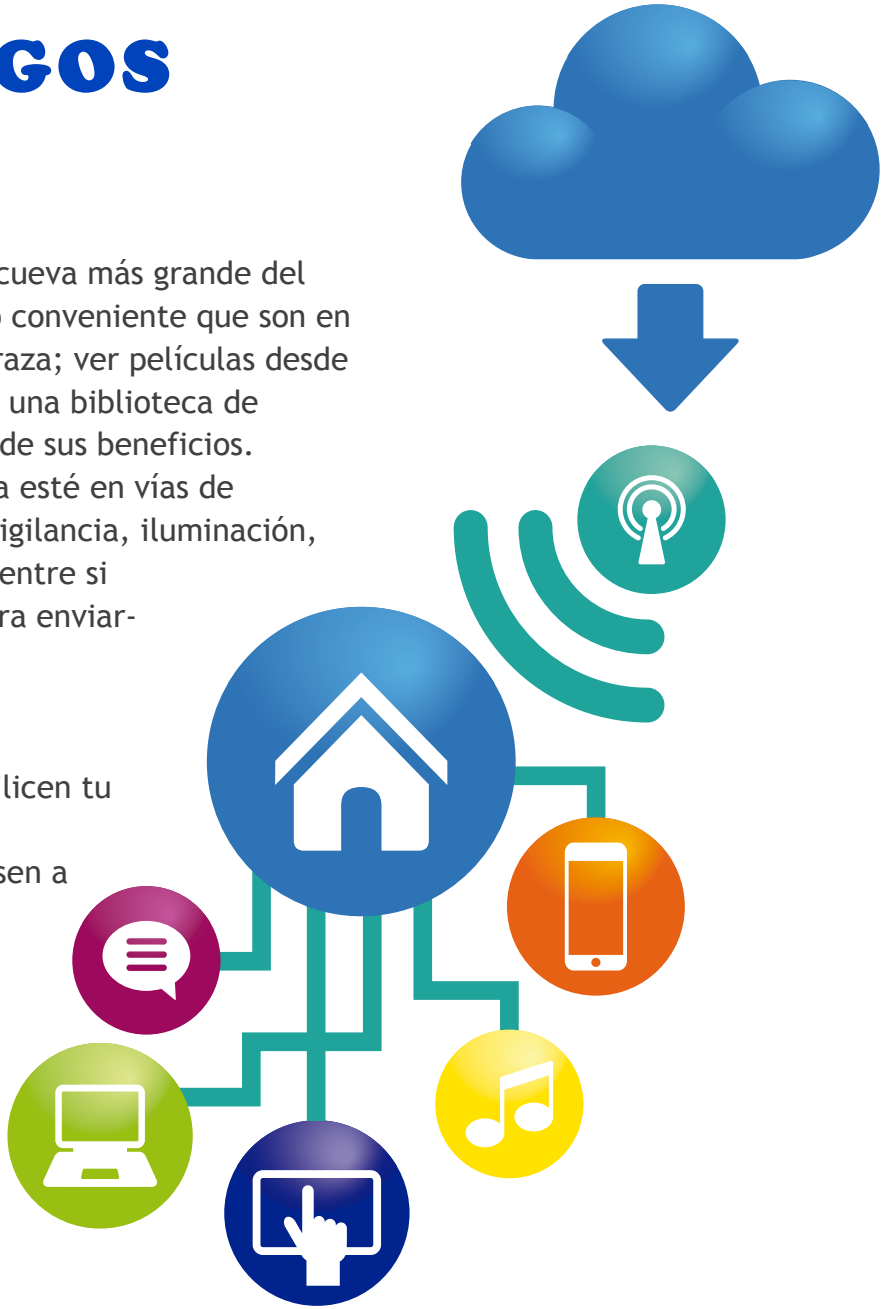
Marzo de 2016

CONTENIDO



RED WI-FI EN CASA:

RED WI-FI EN CASA: CONVENIENCIA Y RIESGOS



Salvo que usted viva en el fondo del mar o en la cueva *Hang Son Doong* (cueva más grande del mundo) en Vietnam, probablemente usted sabe que es una red Wi-Fi y lo conveniente que son en nuestras casas. Conectarse a Internet desde la cocina, habitación o terraza; ver películas desde diferentes dispositivos (smartphone, computadores, *tablets*, etc.), tener una biblioteca de música y compartirla vía *Wireless* con el resto de la familia, son algunos de sus beneficios. Ahora bien, si usted cree en "*Internet of Things*", probablemente su casa esté en vías de convertirse en una casa inteligente donde el sistema de alarma y video vigilancia, iluminación, entretenimiento e inclusive algunos artefactos de cocina, se conectarán entre si automáticamente y a la vez, se conectarán a Internet por redes Wi-Fi para enviar-recibir datos y también generar riesgos.

Los riesgos de una red Wi-Fi poco segura son muchos y permiten a los cibercriminales tomar ventaja. Los riesgos van desde que tus vecinos utilicen tu conexión a Internet gratis (diríamos el menor de los riesgos), hasta que cibercriminales desde cualquier computador conectado a Internet, ingresen a la red Wi-Fi de tu casa, roben tus credenciales de acceso a servicios en línea, vean desde las cámaras cómo se entretienen en las noches o accedan a información confidencial de tus dispositivos digitales.

Por lo antes expuesto, deseamos compartir algunos consejos y buenas prácticas para mejorar la seguridad de red Wi-Fi en casa.

CONSEJOS Y BUENAS PRÁCTICAS

1 * Cambie la contraseña y nombre de usuario enviado por defecto del *router* (*Access Point*).

La contraseña y nombre de usuario de acceso al *router* que viene por defecto, están disponibles en Internet y son conocidas por los cibercriminales. Durante el proceso de instalación del *router*, cambie la contraseña y cree una fuerte de al menos catorce caracteres. Es también sano, cada noventa días cambiar tal contraseña. Si ya tiene una red Wi-Fi y no ha hecho lo indicado aquí, es buen momento para hacerlo.

2 Cambie el SSID por defecto y elimine la opción de que el *router* emita el nombre del SSID.

El SSID (Service Set IDentifier) es un nombre que identifica una red inalámbrica (WLAN), a través del cual diferentes dispositivos se conectan a la WLAN. Los fabricantes de los diferentes router asignan un mismo SSID para sus equipos, el cual al no cambiarse, permitiría a un cibercriminal conocer las vulnerabilidades y acceder a la Wi-Fi de la casa.

Adicionalmente, el router emite una señal constantemente con el nombre del SSID. Eso es lo que aparece en la lista de redes Wi-Fi disponibles en su dispositivo digital. Si bien es cierto para redes Wi-Fi públicas tiene mucho sentido, para redes en casa no, por lo cual, es mejor deshabilitar dicho parámetro.

Configure el protocolo de comunicación segura WPA2-AES.

3

El protocolo WPA2-AES cifra (encripta) la comunicación entre el *router* y el dispositivo digital conectado. Esto ofrece mayor confidencialidad de los datos enviados y recibidos. En caso de que su *router* solo permita utilizar el protocolo inseguro WEP (Wired Equivalent Privacy), es mejor que valore comprar un *router* más moderno.

Deshabilite la administración remota del *router*.

4

Esta función permite, por ejemplo, conectarse desde su oficina al *router* de su casa vía Internet y hacer cambios a la configuración del *router* o ver qué dispositivos están conectados en un momento dado. Lo cierto es que esto también es una puerta de acceso a cibercriminales, los cuales podrían tomar control de su *router* de forma remota.

Deshabilite la opción UPnP si no la necesita.

5

La facilidad UPnP (Universal Plug and Play) permite a diferentes dispositivos conectarse de forma transparente a un *router* y dispositivos entre sí. Esto permitiría a un cibercriminal conectarse fácilmente a la red de la casa e introducir un código malicioso (*malware*) para abrir una puerta de entrada en el *router* de su casa y permitir a terceros no autorizados vía Internet, ingresar a la red. Salvo se tenga una justificación, es mejor deshabilitar esta opción.

6 Mantenga actualizado el software del *router*.

De la misma forma que usted actualiza regularmente los programas antivirus, el software de su *smartphone* o de su computador, debe hacerlo con el *router*. Muchas veces las actualizaciones de los *routers* son para corregir fallas de seguridad. Algunos modelos de *routers* tienen una opción que permita al equipo actualizarse automáticamente. Verifique si su *router* la tiene, pero si no, hágalo usted cada cierto tiempo.

7 Apague el *router* cuando no lo utilice por periodos prolongados.

Si no estará en su casa por varios días o semanas y no requiera conectarse remotamente por Internet a algún dispositivo dentro de la red de su casa, mejor apague el *router*. Además de reducir el riesgo que un cibercriminal se conecte, ayuda a no consumir energía y a la reducción de emisiones de dióxido de carbono.

*Algunos de los consejos de seguridad provienen de las siguientes fuentes:

https://www.us-cert.gov/ncas/tips/ST15-002
https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network
http://www.plus.net/support/broadband/wireless_broadband/secure_home_network.shtml

CONTACTOS

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Raúl Lezcano
t: 279-1410 Ext. 108
rlezcano@riscco.com

riscco.com

Es una compañía panameña, independiente y dedicada, de manera exclusiva, a la consultoría en riesgo tecnológico, seguridad de información y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con siete años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.

Desarrollo Gráfico Bellator Creative SAS
bellatorgallery.com – info@bellatorgallery.com