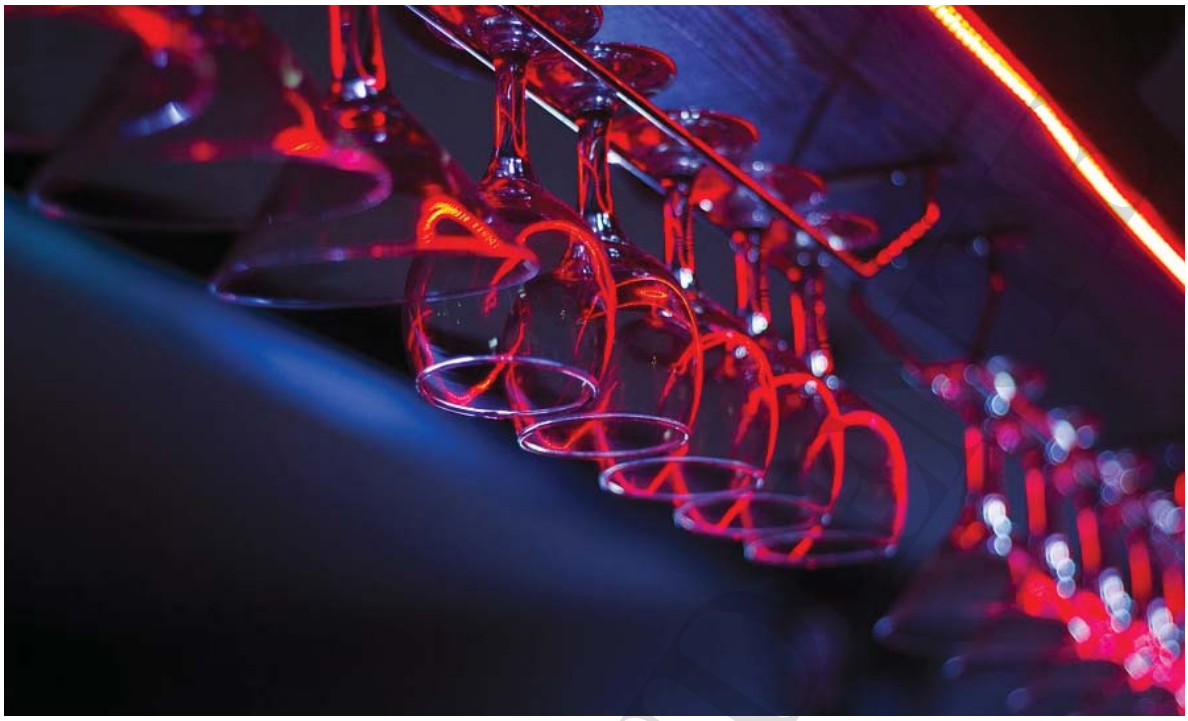
REDES WIFI PÚBLICAS

Extremaremos la precaución a la hora de conectarnos a redes Wi-Fi públicas como las de aeropuertos, bibliotecas, restaurantes y otros lugares públicos para proteger la información que guardamos en nuestros dispositivos móviles. Nos abstendremos de utilizar servicios como la banca online y otros que expongan información sensible.

El principal riesgo es que se trate de una red creada por un particular que intente simular que la suya es la red oficial de, por ejemplo, el aeropuerto para así conseguir que accedan a ella los usuarios. Para evitar esto preguntaremos a los empleados del lugar por el nombre concreto de la red oficial.

Los mayores peligros que conllevan las redes públicas pasan por que los administradores pueden interceptar cualquier acción que realicemos dentro de su red, que nuestra información almacenada en carpetas compartidas quede al alcance de cualquier otro usuario y además que nuestro dispositivo pueda infectarse por algún tipo de malware que albergue la red. Como medida de seguridad adicional procuraremos navegar por webs con protocolo de seguridad https.

EL ESCEPTICISMO ES EL MEJOR CORTAFUEGOS EN LA RED



SALIDAS NOCTURNAS

Los restaurantes, locales comerciales y lugares de ocio pueden ser puntos donde estaríamos más expuestos a ser señalados como objetivos de robo, engaño e incluso secuestro. Aquí, intentaremos no mantener conversaciones sensibles cuando estén cerca los empleados del local.

En las salidas de estos locales y otros lugares muy concurridos las organizaciones criminales utilizan como cómplices a grupos de niños que, aprovechando que piden limosna o venden algo, intentarán sustraernos el teléfono móvil o la documentación que portamos.

Debemos prestar especial atención a las salidas nocturnas y a los lugares de ocio. Estos establecimientos suelen estar controlados por las organizaciones criminales. Las chicas, relaciones públicas y camareros suelen estar en la nómina de estos grupos.

Si se abona la consumición con tarjeta de crédito debemos solicitar al camarero el datáfono para observar in situ la operación. Son muy frecuentes en estos lugares que se utilicen tecnologías de clonación de tarjetas.

EL INDEPEN