

Los principales países con alto riesgo de ciberdelincuencia: Consejos esenciales para viajar de forma segura

06/04/2025



Un reciente estudio de ciberdelincuencia, dirigido por la Dra. Miranda Bruce de la Universidad de Oxford, ha clasificado los países con mayor riesgo en seguridad digital. Este índice revela cuáles son los entornos más hostiles para la privacidad online, destacando la situación de países como Rusia, China e Irán. Si viajas a estos lugares o estás accediendo a sus servicios digitales, necesitas tener en cuenta los riesgos y aprender a proteger tu información personal.

En este artículo, queremos repasar contigo cuáles son algunos de los países más destacados de este índice.

También te ofreceremos nuestra perspectiva sobre los riesgos a los que te expones si usas sus servicios digitales. Por último, te daremos los consejos más importantes para que protejas tu conexión con herramientas como una [VPN para China](#), que evitará males mayores.

Dentro de Europa

1. Rusia – 58,39

El país más peligroso de Europa –y del mundo– en materia digital es Rusia, sobre todo ahora que su invasión

a Ucrania ha disparado la actividad de sus hackers. Rusia ya llevaba tiempo empleando grupos de ciberdelincuentes no solo contra Ucrania, sino también contra otros países considerados enemigos por parte del régimen de Moscú. Sin ir más lejos, el año pasado el FBI desarticuló una herramienta rusa para robar la información de otros gobiernos.

2. Ucrania – 36,44

En respuesta a la invasión de Rusia, Ucrania también ha tenido que hacer uso de grupos de hackers para defenderse digitalmente y tratar de entorpecer los intentos de agresión digital rusos. Algunos de estos hackeos se han llevado a cabo para emitir mensajes en la televisión rusa y trasladar al público lo que está ocurriendo en el frente. Moscú tiene un control férreo sobre la prensa en Rusia, así que la población tiene una opinión sesgada del conflicto.

3. Rumanía – 14,83

En tercer lugar, tenemos a Rumanía, un país que se caracteriza por tener algunas de las sociedades de internet más rápidas del mundo. Tiene una puntuación de 14,83 en este índice, así que también presenta una importante cantidad de hackeos y otros tipos de ciberataques. Aunque se encuentra lejos del riesgo digital de otros países, Rumanía cierra el 'top 3' europeo, así que conviene adoptar las debidas precauciones al viajar a su territorio.

En el resto del mundo

1. China – 27,86

Fuera de Europa, el país con la puntuación más alta es China. Desde hace años hay sospechas de que el gobierno del PCC ha apoyado a hackers para robar información gubernamental o tecnológica en otros países, sobre todo en los Estados Unidos. Además, al viajar a China estaremos tras los 'muros' del Gran Firewall, una herramienta de control estatal que prohíbe el acceso a múltiples plataformas occidentales y monitorea el tráfico online.

2. Estados Unidos – 25,01

Los Estados Unidos no están muy lejos de China en este ranking. Con una puntuación de 25,01, se sitúan como el país más peligroso digitalmente en todo el continente americano. También son el mercado más importante del mundo, así que con frecuencia son el objetivo de hackers y ciberdelincuentes de todo el globo. Esto hace que cualquier transacción online realizada en territorio o webs estadounidenses requiere de fuertes medidas de seguridad digital.

3. Nigeria – 21,28

Finalmente tenemos a Nigeria, considerado el país africano más peligroso en términos de seguridad online. En Occidente, Nigeria se hizo tristemente famosa por una estafa tradicional en la que un supuesto príncipe nigeriano quería repartir su fortuna. Parece ser que esta estafa no se originó en Nigeria en absoluto, así que su puntuación en este índice responde a otros factores: por ejemplo, los hackeos de redes wifi en hoteles y cafeterías.

¿Cómo protegernos?

Al viajar a cualquiera de estos países –o al hacer transacciones en sus páginas web–, siempre conviene tener lista una VPN para cifrar nuestra conexión IP. Para comprobar que la VPN está funcionando podemos conectarnos a un servidor de otro país –por ejemplo, Francia o Italia–, y luego usar una herramienta de localizar IP para geolocalizar la IP. Si nos muestra una IP francesa o italiana, la VPN estará activa y nuestra conexión estará protegida por su cifrado.

Asimismo, suele ser buena idea contar con un buen plan de datos de nuestra tarjeta SIM y evitar las conexiones wifi de las cafeterías o los hoteles. Para conectar el ordenador a internet, podemos abrir un HubSpot desde el móvil y navegar desde él, de modo que nuestra conexión evite por completo redes que podrían ser vulnerables o, directamente, maliciosas. ¡Esto es especialmente importante al hacer pagos digitales para tus reservas de viaje!