



REPORTE NORTON 2013

Octubre, 2013

REPORTE NORTON 2013

¿QUIÉNES PARTICIPARON?

13,022 ADULTOS DE ENTRE 18 Y 64 AÑOS, CONECTADOS A INTERNET

¿DÓNDE? - 24 PAÍSES

AUSTRALIA, **BRASIL**, CANADÁ, CHINA, **COLOMBIA**, DINAMARCA, FRANCIA, ALEMANIA, INDIA, ITALIA, JAPÓN, **MÉXICO**, PAÍSES BAJOS, NUEVA ZELANDA, POLONIA, RUSIA, ARABIA SAUDITA, SINGAPUR, SUDÁFRICA, SUECIA, TURQUÍA, EMIRATOS ÁRABES UNIDOS, REINO UNIDO, ESTADOS UNIDOS

¿A QUIÉNES AFECTA MÁS EL CIBERCRÍMEN? - GLOBAL

PERSONAS CON MÁS PROBABILIDADES DE CONVERTIRSE EN VÍCTIMAS DEL CIBERCRÍMEN :

HOMBRES  – **64%**

(COMPARADO CON 58% DE MUJERES)

MILENIALS / GEN Y – **66%**


(VS. 54% DE LA GENERACIÓN *BABY BOOMERS*)

Y:

- DUEÑOS DE DISPOSITIVOS MÓVILES – **63%**
- USUARIOS DE REDES SOCIALES – **63%**
- USUARIOS DE WI-FI NO SEGURA/ PÚBLICA – **68%**
- MERCADOS EMERGENTES – **68%**
- PADRES DE NIÑOS DE ENTRE 8-17 AÑOS – **65%**

PAÍSES CON MAYOR NÚMERO DE VÍCTIMAS (GLOBAL)** :

 **RUSIA**
85%

 **CHINA**
77%

VS

 **MEXICO**
71%

 **COLOMBIA**
64%

 **BRASIL**
60%



**¿CUÁLES SON LOS PRINCIPALES
HALLAZGOS?**



**MÁS MOVILIDAD
MENOS PROTECCIÓN**

USUARIOS ADOPTAN TABLETAS/SMARTPHONES PERO DEJAN DE LADO LA SEGURIDAD

CASI LA **1/2** DE LOS USUARIOS DE TABLETAS/SMARTPHONES DUERME CON EL TELÉFONO AL ALCANCE DE LA MANO

CASI LA **1/2** NO TOMA LAS PRECAUCIONES BÁSICAS COMO EL USO DE CONTRASEÑAS, SOFTWARE DE SEGURIDAD, O NO REALIZA COPIAS DE SEGURIDAD DE LOS ARCHIVOS DEL DISPOSITIVO*

SOLO **26%** DE LOS USUARIOS DE SMARTPHONES TIENE UN SOFTWARE DE SEGURIDAD EN SU DISPOSITIVO



57% IGNORA QUE EXISTEN SOLUCIONES DE SEGURIDAD PARA LOS DISPOSITIVOS MÓVILES*

CONOCIMIENTO DE LOS USUARIOS SOBRE SEGURIDAD MÁS EN PC Y MENOS EN DISPOSITIVOS MÓVILES

BORRAN CORREOS
SOSPECHOSOS DE
PERSONAS QUE NO
CONOCEN

 **90%**

VS.

 **60%**

VS.

 **56%**

TIENEN AL MENOS UN
ANTIVIRUS BÁSICO
GRATUITO

72%

VS.

42%

VS.

33%

EVITAN GUARDAR
ARCHIVOS
CONFIDENCIALES EN
LÍNEA

78%

VS.

53%

VS.

48%



DISPOSITIVOS MÓVILES: CIBERCRÍMEN Y PÉRDIDAS

38% HA SUFRIDO UN DELITO INFORMÁTICO EN
LOS ÚLTIMOS 12 MESES *

27% DE LOS ADULTOS HA PERDIDO SU
DISPOSITIVO MÓVIL O SE LO HAN ROBADO





COSTO GLOBAL DEL CIBERCRIMEN

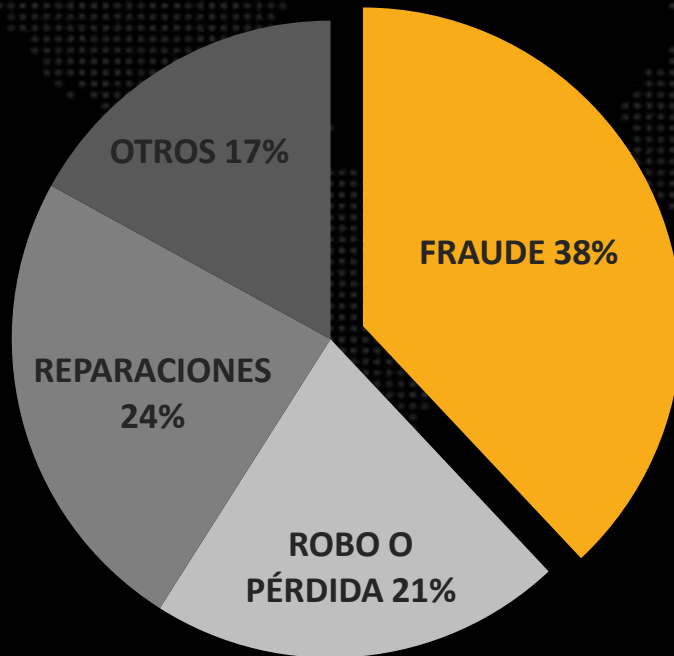
EL COSTO GLOBAL DEL CIBERCRÍMEN

\$113 MM

SUFICIENTE PARA DAR USD\$194 A CADA
CIUDADANO DE AMÉRICA LATINA



EL 83% DE LOS COSTOS FINANCIEROS
DIRECTOS SON EL RESULTADO DE FRAUDE,
REPARACIONES, ROBOS Y PÉRDIDAS



USD \$298

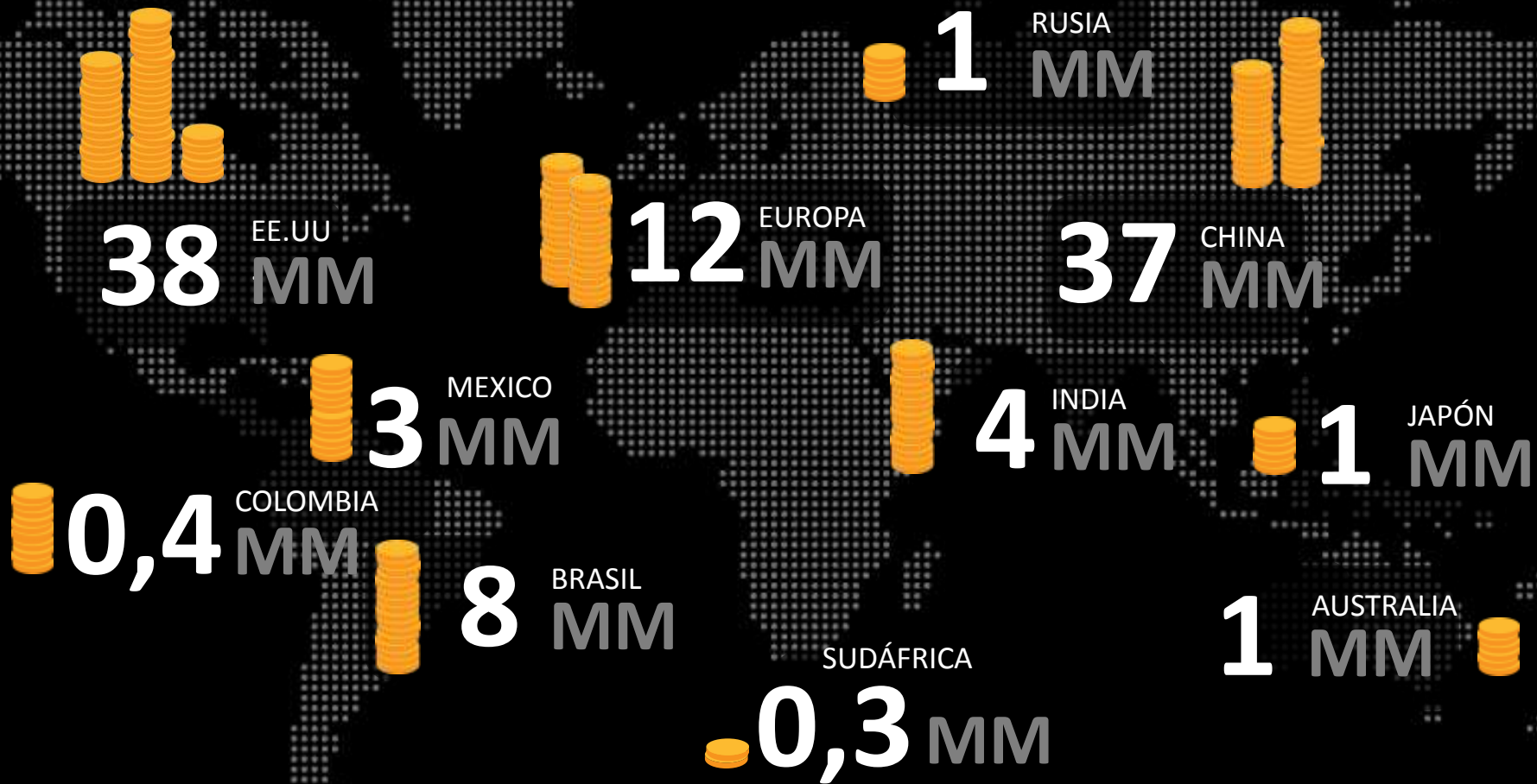
COSTO PROMEDIO POR VÍCTIMA

REPRESENTA UN 50% MÁS QUE EN EL 2012

TODOS LOS MONTOS EN DÓLARES ESTADOUNIDENSES

VER CÁLCULOS POR EXTRAPOLACIÓN*

EL COSTO MUNDIAL DEL DELITO INFORMÁTICO AL CONSUMIDOR



TODOS LOS MONTOS EN USD SE APROXIMARON AL MM MÁS CERCANO

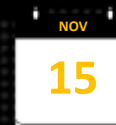
CANADÁ 3 MM; SINGAPUR 1 MM; NUEVA ZELANDA 0,1 MM; TURQUÍA 2 MM; ARABIA SAUDITA 0,5 MM; EAU 0,3 MM; COLOMBIA 0,5 MM



ESCALA DEL CIBERCRIMEN

LA ESCALA DEL CIBERCRÍMEN

378 MILLONES DE VÍCTIMAS POR AÑO



CASI EL TOTAL DE HABITANTES DE AMÉRICA DEL SUR



1 MILLÓN +
VÍCTIMAS POR DÍA

SUFICIENTE PARA LLENAR CASI 13 VECES EL ESTADIO MARACANÁ DE BRASIL



12 VÍCTIMAS POR SEGUNDO

LA ESCALA DEL CIBERCRÍMEN



50% DE LOS ADULTOS

HA SIDO VÍCTIMA DE UN DELITO INFORMÁTICO Y/O DE UN INCIDENTE EN LÍNEA EN EL ÚLTIMO AÑO
(Ej: RECIBIÓ FOTOS DE DESNUDOS O SUFRIÓ ACOSO CIBERNÉTICO)

41% DE LOS ADULTOS

CONECTADOS A LA RED HA SUFRIDO ATAQUES TALES COMO MALWARE, VIRUS, PIRATERÍA, ESTAFAS, FRAUDES Y ROBO





**LA DELGADA LÍNEA ENTRE LO
PERSONAL Y LABORAL**

LA DELGADA LÍNEA ENTRE TRABAJAR Y JUGAR



49%

USA SU DISPOSITIVO MÓVIL PARA TRABAJAR Y JUGAR*

49%

REVISA O ENVÍA EMAILS
PERSONALES DESDE SU
DISPOSITIVO DE
TRABAJO*

34%

ENTRA A REDES
SOCIALES EN SU
DISPOSITIVO DE
TRABAJO*

27%

ALMACENA
INFORMACIÓN PERSONAL
EN SU DISPOSITIVO DE
TRABAJO*

30%

**DE LOS PADRES DEJA A SUS HIJOS JUGAR, DESCARGAR Y
REALIZAR COMPRAS DESDE SU DISPOSITIVO DE TRABAJO****

36%

**DICE QUE LA EMPRESA DONDE TRABAJA NO TIENE
POLÍTICAS QUE REGULEN EL USO DE DISPOSITIVOS PERSONALES EN
EL TRABAJO***

*ENTRE ADULTOS TRABAJADORES

**ENTRE PADRES QUE USAN DISPOSITIVOS PROPORCIONADOS POR EL EMPLEADOR

EL ALMACENAMIENTO ONLINE ABRE LA PUERTA AL OVERSHARING

24% DE LOS USUARIOS GUARDA DOCUMENTOS
LABORALES Y PERSONALES EN LA MISMA CUENTA DE
ALMACENAMIENTO EN LÍNEA



COMPARTEN INFORMACIÓN RELACIONADA CON EL TRABAJO A
TRAVÉS DE SITIOS DE ALMACENAMIENTO EN LÍNEA:

18% COMPARTE CON AMIGOS

21% COMPARTE CON SU FAMILIA

**LA INFORMACIÓN LABORAL Y PERSONAL
EN RIESGO**

EN RESUMEN

50% DE LOS ADULTOS

**CONECTADOS A LA RED HA SIDO VÍCTIMA
DE UN CIBERDELITO Y/O HA SUFRIDO
INCIDENTES EN EL ÚLTIMO AÑO**

TODOS LOS DÍAS, MÁS DE 1 MILLÓN DE ADULTOS ES
VÍCTIMA DE DELITOS INFORMÁTICOS, ES DECIR, 12 VÍCTIMAS
POR SEGUNDO

US\$113

MIL MILLONES

**COSTOS DIRECTOS GLOBALES
TOTALES EN SOLO 12 MESES**

- 1. LOS CONSUMIDORES USAN DISPOSITIVOS MÓVILES
PERO NO LE DAN IMPORTANCIA A LA SEGURIDAD**
- 2. DISPOSITIVO MÓVIL PERSONAL Y DE TRABAJO**
- 3. LOS CONSUMIDORES ELIGEN CONVENIENCIA POR
SOBRE SEGURIDAD**

5 CONSEJOS PARA REDUCIR LOS RIESGOS

PROTEGER LOS DATOS

UN PAQUETE INTEGRAL DE SEGURIDAD BRINDA UNA SÓLIDA DEFENSA CONTRA LAS AMENAZAS CIBERNÉTICAS. NORTON 360 MULTI-DISPOSITIVO OFRECE PROTECCIÓN COMPLETA PARA COMPUTADORAS, SMARTPHONES Y TABLETAS, TODO EN UNA MISMA SOLUCIÓN

LOS DISPOSITIVOS MÓVILES SON COMO MINI COMPUTADORAS

LOS DISPOSITIVOS MÓVILES SE HAN TRANSFORMADO RÁPIDAMENTE EN EL OBJETIVO DE LOS DELINCUENTES INFORMÁTICOS. ASEGÚRESE DE PONER CONTRASEÑA A SUS DISPOSITIVOS, Y TOME LAS MEDIDAS NECESARIAS PARA GARANTIZAR LA PROTECCIÓN CONTRA ROBO, PÉRDIDA O DELITO INFORMÁTICO

CUIDADO EN LA NUBE

SI BIEN LAS SOLUCIONES DE ALMACENAMIENTO EN NUBE AYUDAN A GUARDAR Y COMPARTIR ARCHIVOS, SON UNA PUERTA DE ACCESO PARA LOS ATAQUES INFORMÁTICOS. PRESTE ATENCIÓN A QUIENES TIENEN ACCESO A SUS ARCHIVOS, Y EN LO POSIBLE UTILICE UNA SOLUCIÓN CON PROTECCIÓN INCORPORADA.

OPERACIONES CONFIDENCIALES CON CONEXIONES SEGURAS

LAS REDES DE WI-FI LIBRES O NO SEGURAS PUEDEN AYUDAR A LOS LADRONES A ESPIAR SUS ACTIVIDADES. EVITE REALIZAR TRANSACCIONES CON INFORMACIÓN CONFIDENCIAL, COMO BANCARIAS O COMERCIALES, MIENTRAS ESTÁ CONECTADO A ESTAS REDES, O UTILICE UN CLIENTE VPN PERSONAL

DESPUÉS DE CONECTARSE, REVISE TODO

REVISE LOS RESÚMENES BANCARIOS Y DE SU TARJETA DE CRÉDITO CON FRECUENCIA PARA DETECTAR TRANSACCIONES FRAUDULENTAS, E INFORME CUALQUIER ACTIVIDAD SOSPECHOSA A SU PROVEEDOR Y/O A LOS AGENTES DE SEGURIDAD CORRESPONDIENTES



¡GRACIAS!

Más Información:

www.symantec.com/la/reportenorton



Norton[™]
by Symantec



ANEXO



**¿QUÉ ENTENDEMOS COMO
DELITO INFORMÁTICO?**

DEFINICIÓN DE DELITO INFORMÁTICO

Se entiende por delito informático alguna de estas actividades:

- Apareció un virus o un malware en mi computadora.
- Respondí un correo electrónico fraudulento, 'engañoso' o falso, o ingresé a un sitio web que capturó mis datos personales (mis contraseñas, número de tarjeta de crédito o información sobre mi cuenta bancaria) pensando que era una solicitud válida con el fin de tener acceso a información o brindar datos a una organización legítima, como por ejemplo mi entidad bancaria, etc.
- Alguien hackeó mi casilla de email y se hizo pasar por mí.
- Alguien hackeó mi perfil de red social y se hizo pasar por mí.
- Respondí a una estafa en línea.
- He sufrido un fraude con tarjeta de crédito en línea.
- He sufrido el robo de identidad.
- Mi teléfono celular fue infectado y se envió un mensaje de texto desde mi equipo sin mi permiso ni conocimiento, que luego tuve que pagar.
- Se bloqueó la pantalla de mi teléfono celular y apareció una alerta que exigía el pago de una multa para desbloquearla.
- Extravié o me robaron mi smartphone, alguien lo encontró y lo utilizó sin mi permiso.
- Apareció una aplicación en mi smartphone que yo no había descargado.
- Recibí una llamada que supuestamente era de una empresa de informática, en la que me informaban que mi computadora estaba infectada.
- Sufrí otro tipo de delito informático en mi teléfono celular / dispositivo móvil / tableta.
- Sufrí otro tipo de delito informático en mi computadora de escritorio / portátil.

DEFINICIÓN DE DELITO INFORMÁTICO

El ciberdelito y/o incidente en línea se define como alguna de las siguientes actividades:

- Apareció un virus o un programa maligno en mi computadora.
- Respondí un correo electrónico fraudulento, 'engañoso' o falso, o ingresé a un sitio web que capturó mis datos personales (mis contraseñas, número de tarjeta de crédito o información sobre mi cuenta bancaria) pensando que era una solicitud válida con el fin de tener acceso a información o brindar datos a una organización legítima, como por ejemplo mi entidad bancaria, etc.
- Alguien hackeó mi casilla de email y se hizo pasar por mí.
- Alguien hackeó mi perfil de red social y se hizo pasar por mí.
- Respondí a una estafa en línea.
- He sufrido un fraude con tarjeta de crédito en línea.
- He sufrido el robo de identidad.
- Mi teléfono celular fue infectado y se envió un mensaje de texto desde mi equipo sin mi permiso o conocimiento, que luego tuve que pagar.
- Se bloqueó la pantalla de mi teléfono celular y apareció una alerta que exigía el pago de una multa para desbloquearla.
- Extravié o me robaron mi smartphone, alguien lo encontró y lo utilizó sin mi permiso.
- Apareció una aplicación en mi smartphone que yo no había descargado.
- Recibí una llamada que supuestamente era de una empresa de informática, en la que me informaban que mi computadora estaba infectada.
- Sufrí otro tipo de delito informático en mi teléfono celular / dispositivo móvil / tableta.
- Sufrí otro tipo de delito informático en mi computadora de escritorio / portátil.
- Alguien publicó fotos o videos privados/íntimos míos sin mi autorización.
- Alguien me contactó en línea de manera sexual e inapropiada.
- Sufrí acoso, abuso, discriminación cibernéticos u otro tipo de hostigamiento en línea.
- Recibí mensajes de texto de personas que no conozco, solicitándome hacer clic en un enlace o diciendo que recibí un mensaje de voz y que debo marcar un número que no es el que corresponde a mi casilla de voz.
- Recibí imágenes no deseadas de personas desnudas de parte de un desconocido.
- Recibí imágenes no deseadas de personas desnudas de parte de alguien que conozco.



METODOLOGÍA

DETALLES DE LA METODOLOGÍA UTILIZADA

EDELMAN BERLAND REALIZÓ UNA ENCUESTA EN LÍNEA ENTRE SUS CONSUMIDORES:

13.022 ADULTOS DE ENTRE 18 y 64 AÑOS

La encuesta fue realizada en 24 países (Australia, Brasil, Canadá, China, Colombia, Francia, Dinamarca, Alemania, India, Italia, Japón, México, Países Bajos, Nueva Zelanda, Polonia, Rusia, Arabia Saudita, Singapur, Sudáfrica, Suecia, Turquía, Emiratos Árabes Unido, Reino Unido y Estados Unidos)

Se realizó en el idioma oficial de cada país, y las preguntas formuladas fueron idénticas en todos los países.

Las entrevistas se llevaron a cabo entre el 4 de julio de 2013 y el 1 de agosto de 2013.

El margen de error para la muestra total de adultos (n=13.022) es + 0,9% con un nivel de confianza del 95%.

Observaciones importantes:

El Informe de Norton sobre delitos informáticos es un informe anual pedido por Norton by Symantec, cuyo objetivo

es entender cómo los delitos informáticos afectan a los consumidores y cómo la adopción y evolución de las nuevas tecnologías impacta sobre la seguridad de los usuarios. La investigación estuvo a cargo de Edelman Berland, una agencia de investigación a nivel mundial. Los resultados se obtuvieron en base a la experiencia (informada por ellos mismos) de más de 13.000 adultos en 24 países.

1.000 de los adultos encuestados fueron entrevistados en EE.UU. y la India. Los datos globales se ponderaron para garantizar que todos los países tuviesen la misma cantidad de participantes, n=500 adultos.

Observaciones adicionales:

Mercados Desarrollados: EE.UU, Canadá, Reino Unido, Francia, Alemania, Italia, Suecia, Países Bajos, Australia, Japón, Singapur, Nueva Zelanda, Dinamarca.

Mercados Emergentes: Brasil, México, Polonia, India, China, Rusia, Turquía, Arabia Saudita, Emirato Árabes Unidos, Colombia, Sudáfrica.

Generación Y: entre 18 y 34 años

Baby Boomers: entre 45 y 64 años

CÁLCULOS POR EXTRAPOLACIÓN

1) Casi 380 millones de víctimas en 24 países

Los adultos conectados a la red por país x % víctimas de delitos informáticos en los últimos 12 meses por país = 377.943.431 (suma de 24 países).

2) 12 víctimas de delitos informáticos por segundo / 719 víctimas por minuto / 43.144 por hora / más de 1 millón por día, lo que da un total de casi 378 millones de adultos en el último año en 24 países*

Víctimas en los últimos 12 meses (como se indica arriba)
377.943.431 / 365 días por año / 24 horas / 60 minutos / 60 segundos

3) El delito informático es un gran negocio: tuvo un costo de USD 113 mil millones en el último año en un total de 24 países

Las víctimas en los últimos 12 meses (por país) x costo financiero promedio de cada delito (por país, en USD). La cifra se muestra en la suma del costo total de todos los países.