CIBERSEGURIDAD.com

El perito informático como nuevo perito caligráfico.

Riesgos de los sistemas de mensajeria en el ámbito familiar

Luis Vilanova Blanco – Perito judicial

Agenda

Ciberseguridad.com

Email

Whatsapp

Otros sistemas de mensajeria

Preguntas

PROFESIONALES INDEPENDIENTS DE LA SEGURIDAD DE SU INFORMACIÓN

Ciberseguridad.com se sitúa como uno de las principales consultoras de ciberseguridad, peritaje judicial y auditoria ISO27001 a nivel nacional, realizando proyectos para Ministerio de Industria, Colaborando con la justicia y realizando planes directores de seguridad, junto con hacking ético en muchas empresas nacionales e internacionales.

Peritos y auditores informáticos colaboradores con la justicia a nivel nacional.

Miembros de diferentes asociaciones de peritaje y auditoria, así como de comités de dirección.

Auditores Cloud SaaS para el Ministerio de Industria red.es

Auditores independientes ISO27001, ITIL y gobierno TI con mas de 20 años de experiencia, con oficinas en Madrid y Valencia.

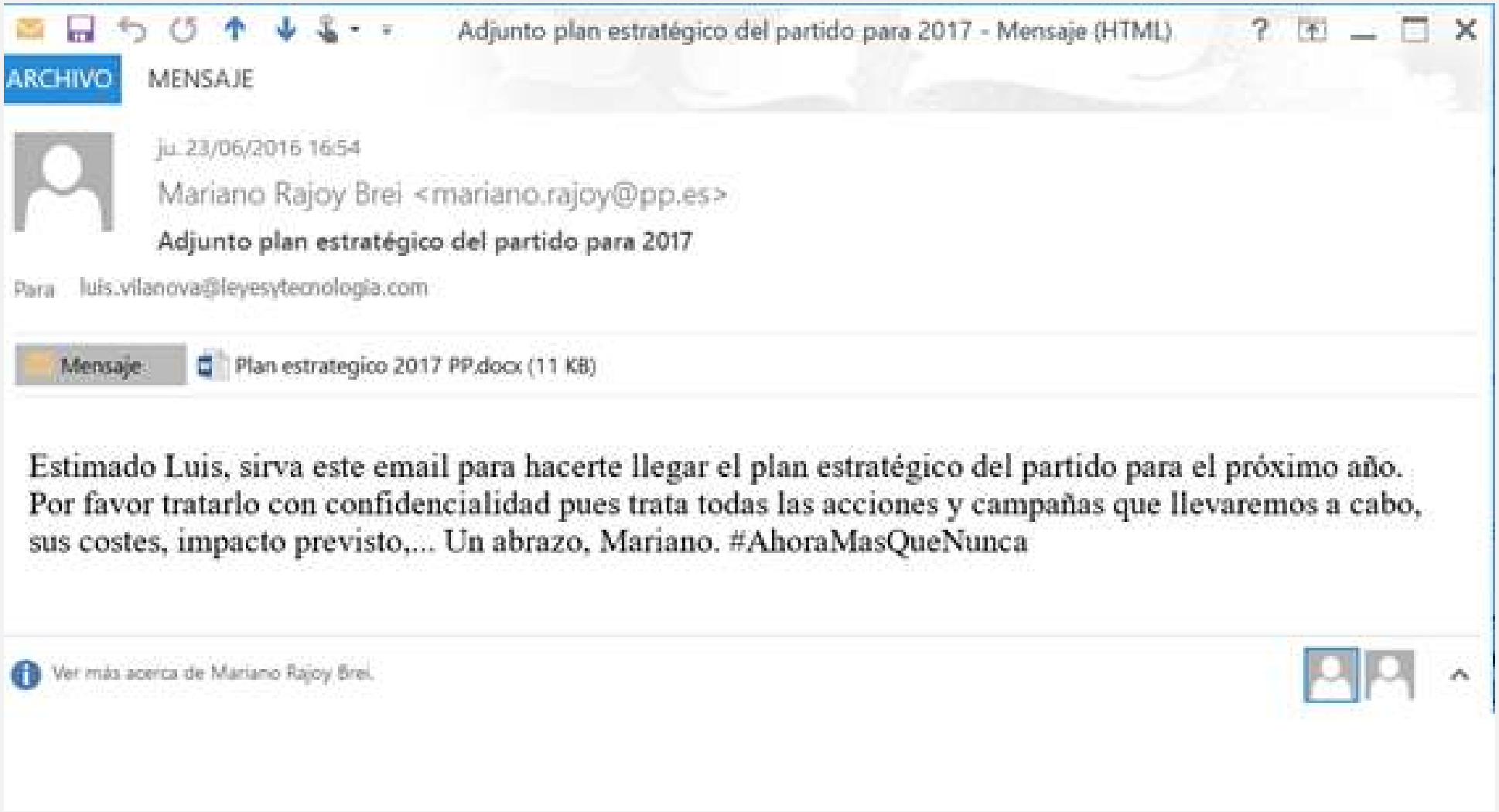
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
EOI Escuela de organización industrial

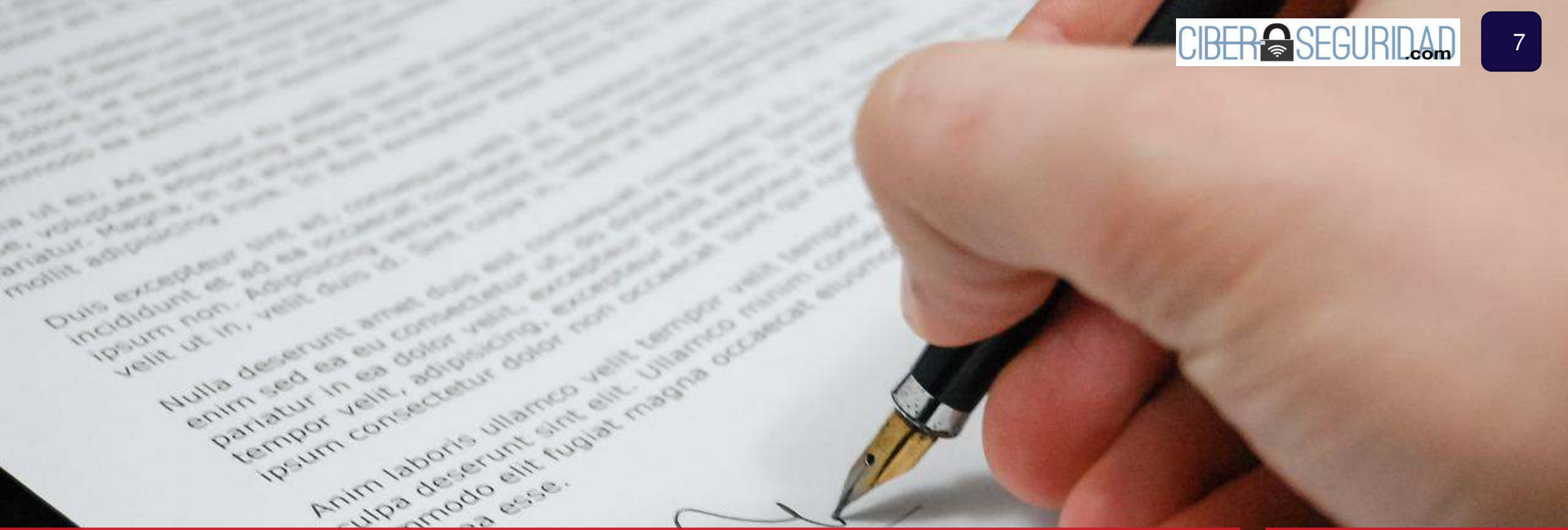
Profesores homologados

Auditoría de ciberseguridad, peritaje informático y hacking ético.

Email

- Sistema antiguo
- Excasa seguridad
- Facilmente falsificable
- En ocasiones no se conserva el original
- Pueden ser utilizados origenes dificilmente rastreables o intervenibles

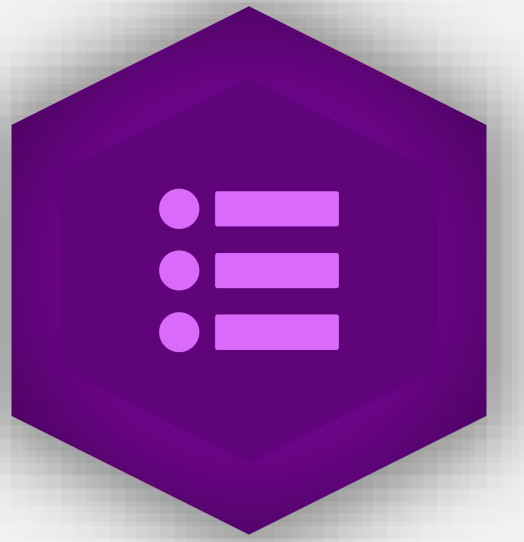

Adjunto plan estratégico del partido para 2017 - Mensaje (HTML)
ARCHIVO
MENSAJE
ju. 23/06/2016 16:54
Mariano Rajoy Brei <mariano.rajoy@pp.es>
Adjunto plan estratégico del partido para 2017
Para luis.vilanova@leyesytecnologia.com
Mensaje
Plan estrategico 2017 PP.docx (11 KB)
Estimado Luis, sirva este email para hacerte llegar el plan estratégico del partido para el próximo año. Por favor tratarlo con confidencialidad pues trata todas las acciones y campañas que llevaremos a cabo, sus costes, impacto previsto,... Un abrazo, Mariano. #AhoraMasQueNunca
Ver más acerca de Mariano Rajoy Brei.



Metadatos

Email - Metadatos

Son datos que llevan implicitos los emails y que nos ayudan a demostrar el origen, destino, cuerpo, adjuntos, destinatarios, fecha y hora y no alterabilidad*



Los metadatos pueden llegar a ser alterados sin dejar rastro a no ser que se envie con firmas seguras como gmail.

Si no accedemos al email original no es possible disponer de ellos

Return-path: <comunicacion@asoper.es>
Envelope-to: luis.vilanova@leyesytecnologia.com
Delivery-date: Sat, 10 Sep 2016 12:21:57 -0500
Received: from [184.154.177.50] (port=60788 helo=se7.mailspamprotection.com)
by siteground198.com with esmtps (TLSv1.2:ECDHE-RSA-AES256-SHA:256)
(Exim 4.86_2)
(envelope-from <comunicacion@asoper.es>)
id 1bilyW-0008IU-Vr
for luis.vilanova@leyesytecnologia.com; Sat, 10 Sep 2016 12:21:56 -0500
Received: from smtpcmd0995.aruba.it ([62.149.156.95])
by se7.mailspamprotection.com with esmtp (Exim 4.85)
(envelope-from <comunicacion@asoper.es>)
id 1bilyT-000270-Gm
for luis.vilanova@leyesytecnologia.com; Sat, 10 Sep 2016 12:21:56 -0500
Received: from PCToshibaHome ([90.94.85.230])
by smtpcmd09.ad.aruba.it with bizsmtp
id htMp1t00N4yAXma01tMqYh; Sat, 10 Sep 2016 19:21:51 +0200
MIME-Version: 1.0
From: =?utf-8?Q?Asociaci=C3=B3n_Profesional_Colegial_de_Peritos_Judiciales_?=<comunicacion@asoper.es>
Reply-To: comunicacion@asoper.es
To: luis.vilanova@leyesytecnologia.com
Content-Type: multipart/related;
type="text/html";
boundary="----=_NextPart_001_1EB5_1A216321.6B882893"
X-Mailer: Smart_Send_3_1_0
Date: Sat, 10 Sep 2016 19:21:50 +0200
Message-ID: <25803427302881161728438@PC-Toshiba>
X-Filter-ID: s0sct1PQhAABKnZB5plbId85UEVE1G8/J5IO7pEpLoIZWJmBXpDNTqXr/4FInY8NwS9kmloc0QPc
6NojePGshHmkIdwxi0OxAm0KXrLnlCz/LlIAwXw7oHXL0hU1/g4/9et9DHQyRSwjtwH3Ay7gBtBM
V4xVJlZORXN0dRz/FabkuzfD3DfDDJZTnNtwRohbwo009VZeylSo1IExeDu1Xkph+MKbCLSsuGrt
LclqiLRNz4V5+SBdfv/5J7zFY1GIUQV07+bGJw1XTktCLBQSMGbjO41FyBEqIaDudcVplPHr2Be/
h7aa8ON7WgtYEjC5Otsh1sqkwMirfq6RxjzZSCzcdn4RlD0lmHgBHUxTXSF6PH5kQfzcPe5Psb29
XFKgokU4FB3/7dMmssMHUmCLGuuO5TcDeKjrEmYPn2IVWRsTqgbTTDPTUTZQjM3MDuQijs+TgHFQ
Ax7SkhJEM3JHOeikA053AiEzBuBvUBrAqVELxN0Dm6+b5joKnx+pjyIFWMqaPqFzEMTwH7TEN9A4
LAfP9Vy8irEwta0V6dwmff0E/Xy9bqh2t87xwDNJ1ZQnZjZlKwEfjW95SXJLOI0iUkCbSNTtgnWe

Sat, 10 Sep 2016 12:21:57
From: =?utf-8?Q?Asociaci=C3=B3n_Profesional_Colegial_de_Peritos_Judiciales_?=<**comunicacion@asoper.es**>
Reply-To: comunicacion@asoper.es
To: **luis.vilanova@leyesytecnologia.com**
Content-Type: multipart/related;

Desprotección sin SSL

Aportación en un juicio

Disponer del original o poder tener acceso al servidor donde

se emitió es fundamental, pues es la fuente de los metadatos fiables

En ocasiones el cliente no tiene el email original

No tiene acceso al servidor origen

No existe copia de seguridad del email

Fue un reenvío a un grupo y no podemos asegurar su veracidad

Rara vez se discute en un juicio la veracidad de un email donde un perito informático a estudiado al máximo los metadatos que en el se encuentran.

Derecho de familia

Los emails mas communes en este tipo de juicios son para amenazar a alguna parte y reclamar dinero.

Amenazas

En deudas familiares reclamadas por email

En divorcios, separaciones, custodias compartidas,…

Recientemente en un caso de ruptura y deuda

Whatsapp

Whatsapp

LIDER

Utilizado en millones de dispositivos

SEGURO

Transmisión encriptada desde hace unas pocas versiones

OPORTUNIDAD

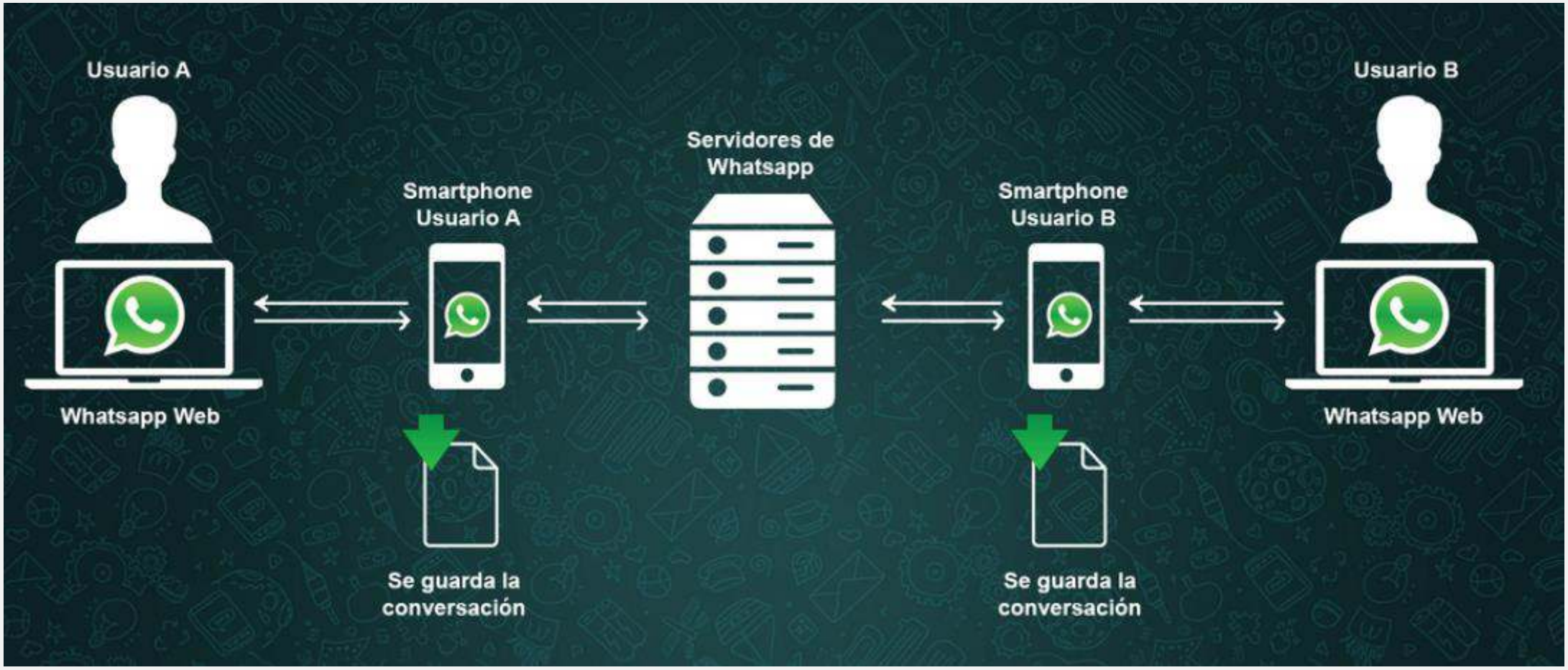
Para expresar todo tipo de sentimientos.

RIESGO

No se almacena nada en ningun servidor

Información

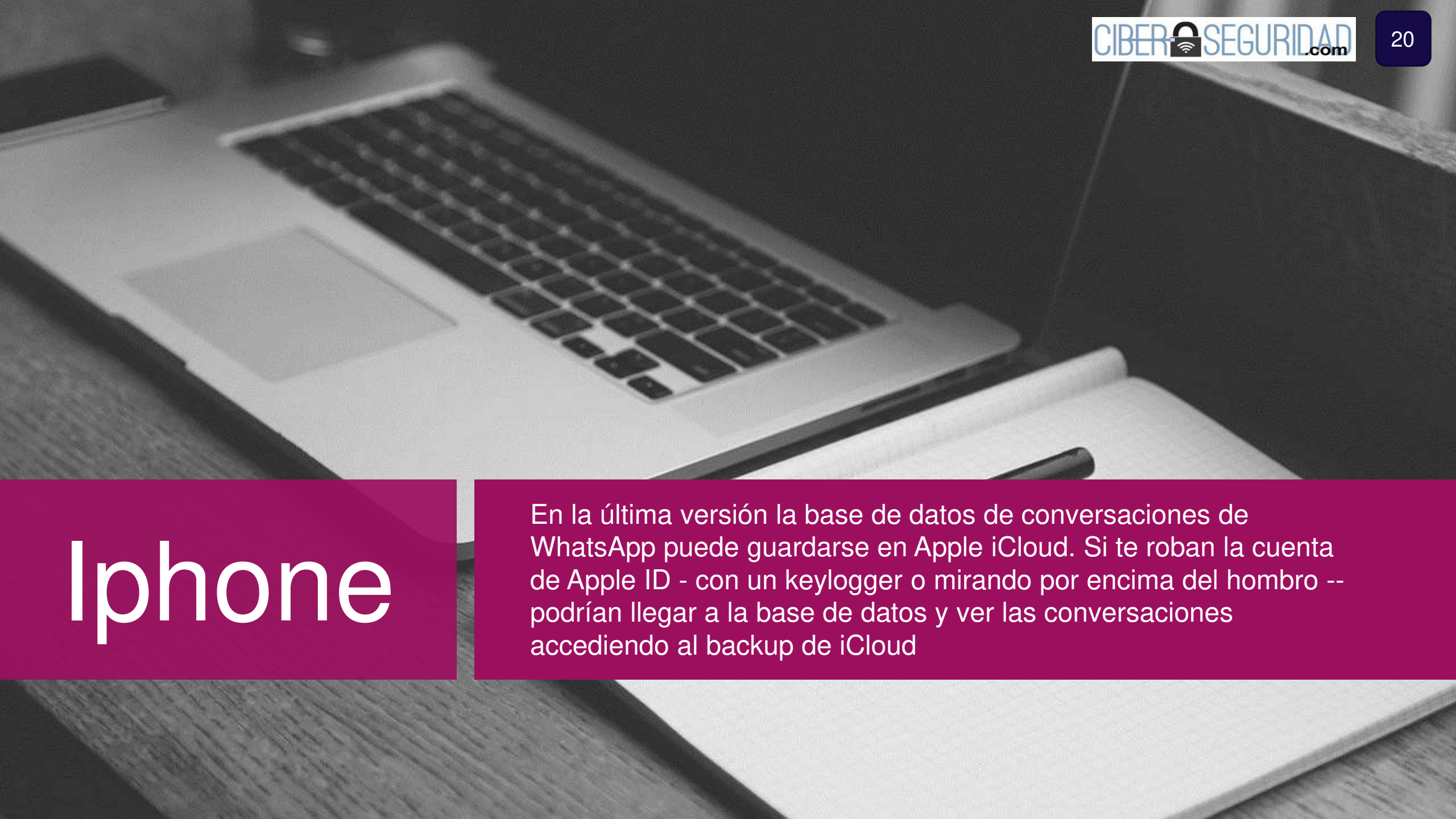
La información es almacenada en el dispositivo en una base de datos encriptada y otra sin encriptación


Usuario A
Usuario B
Servidores de Whatsapp
Smartphone Usuario A
Smartphone Usuario B
Whatsapp Web
Whatsapp Web
Se guarda la conversación
Se guarda la conversación

Algunas cuestiones

Privacidad

Acceso completo

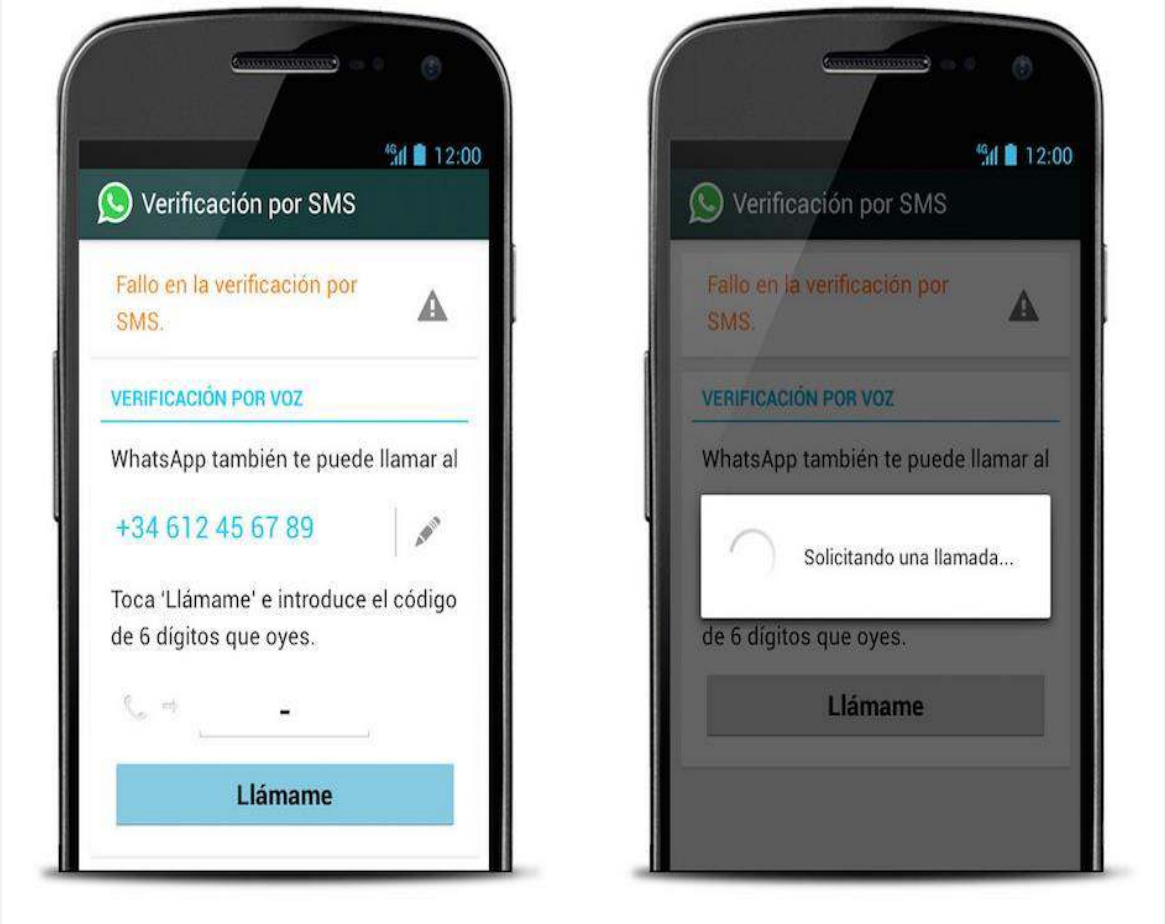


Iphone

En la última versión la base de datos de conversaciones de WhatsApp puede guardarse en Apple iCloud. Si te roban la cuenta de Apple ID - con un keylogger o mirando por encima del hombro -- podrían llegar a la base de datos y ver las conversaciones accediendo al backup de iCloud

Se puede obtener la base de datos de WhatsApp de la SDCard. Esta base de datos tiene un cifrado muy sencillo de quitar para obtener después el fichero SQLite en plano. Si se sube la base de datos cifrada a Recover Messages, se obtiene la base de datos descifrada automáticamente de forma gratuita. En los últimos resultados, ya hay más de 800.000 bases de datos analizadas con Recover Messages, y más de 25.500 usuarios registrados.

Android



Espiar WhatsApp con robo de cuenta con acceso físico al teléfono

1. Teléfono cerca y previsualización de mensajes SMS
2. Instalar Whatsapp en tablet
3. Pedir SMS de confirmación (o voz)

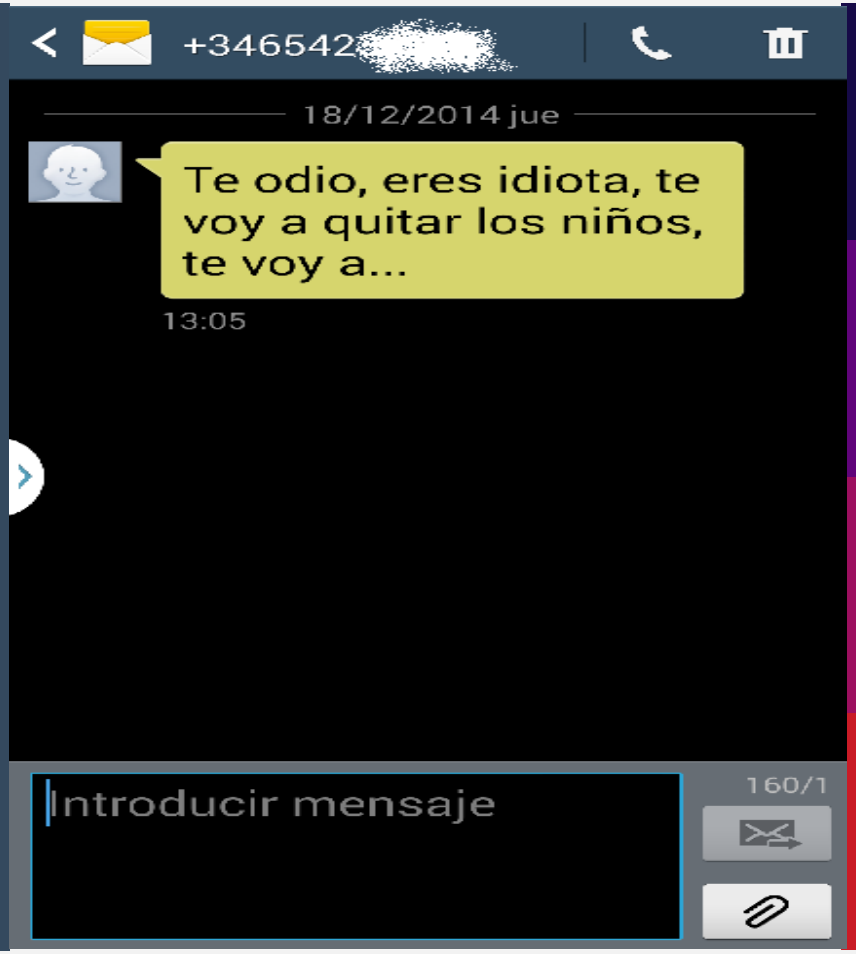
Usemos un troyano

Muchos programas, APP, juegos, etc pueden seconder un software mailicioso que aparentemente no lo es y que una vez instalado puede estar en ejecución sin mostrar ninguna evidencia aparente.

SMS

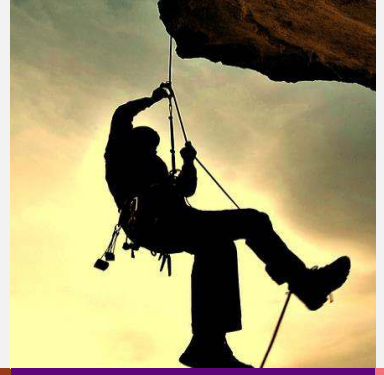
FALSO

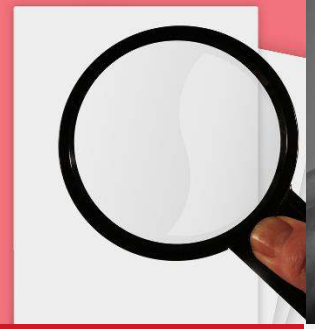
De fácil falsificación aparente



- El coste de falsificarlo es cero
- Alta calidad de la falsificación
- Suplantación de otros numeros
- Difícil rastreo

Nuestro trabajo





Es importante contactar cuanto antes con un perito informático en cuanto detectamos alguna evidencia.
EL TIEMPO DE RESPUESTA ES VITAL

Metodología

Cadena de custodia

Fase I: Obtener el original

Aislar a prueba

Análisis

Fase II: Auditoria

Determinar o demostrar no alterabilidad

Evidencias

Fase III: Extracción

Obtener las pruebas y documentarlas

Fase IV: Defensa

Defensa oral ante el juez

Vista oral

..y entonces?

Ley de Enjuiciamiento Criminal en su artículo 579 de 22 de septiembre de 2015, deja libertad para considerar la validez de la prueba, no entrando a valorar si este medio puede generar dudas, o no.

Varias sentencias fallan a favor de la prueba de Whatsapp, como la Sentencia 180/2011, de la Audiencia Provincial de Las Palmas, en la que no se acepta la posibilidad de que "…la mera protesta de que el whatsapp es manipulable y de que las conversaciones pudieron ser mantenidas por el anterior titular, es manifiestamente insuficiente para alterar la valoración probatoria en el sentido interesado en el recurso…"

El profesional forense que extraiga la prueba del móvil intervenido, deberá igualmente certificar que el terminal no ha sido rooteado, ni manipulados los privilegios de ciertos directorios, a mayores de la necesaria certificación y protección de los ficheros de whatsapp y su contenido

Recomendaciones a las familias

Activar siempre los mecanismos de log comprobando periodicamente quien accede desde donde y desde que dispositivos.

Actualizar el Sistema a la ultima versión

Ocultar la ubicacion

Adquirir software de seguridad

Educación a los niños y familiars de los riesgos

Muchas gracias

Los sistemas de mensajeria en general no son seguros, en su concepción o por ingenieria social. Actuemos!

info@ciberseguridad.com

www.ciberseguridad.com

911277300