



## Lo bueno, lo malo y lo feo de las nuevas regulaciones en Seguridad de la Información en México

Jorge Osorio – Director de Servicios de Consultoría

CISSP – CEH – ITIL

# Cae el H1 en operativo contra hackers; estaría detrás del ataque al SPEI

Se catearon once domicilios y aseguraron 27 vehículos de lujo, motocicletas, cajas fuertes, con un total de 20 millones de pesos en efectivo cada una, armas y droga



Héctor Ortiz Solares, alias "El H1" o "El Patrón", el criminal más buscado en México.



## LO ASEGURADO

- \*27 autos de lujo
- \*2 cuatrimotos
- \*4 motocicletas
- \*2 armas de fuego
- \*9 cajas de plástico con dinero en efectivo con un monto cercano a los 20 millones 442 mil 239 pesos.
- \*Dosis de marihuana, cocaína y cristal
- \*15 equipos de cómputo
- \*29 teléfonos celulares, 4 dispositivos USB y discos duros.
- \*1 uniforme con la leyenda Policía Federal.
- \*Documentos diversos
- \*Un portafolio.

## Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019

Applies to: Security, Windows

Microsoft is aware that some customers are running versions of Windows that no longer receive mainstream support. That means those customers will not have received any security updates to protect their systems from CVE-2019-0708, which is a critical remote code execution vulnerability.

Given the potential impact to customers and their businesses, we made the decision to make security updates available for platforms that are no longer in mainstream support (see download links in the following table). These updates are available from the Microsoft Update Catalog only. We recommend that customers running one of these operating systems download and install the update as soon as possible.

Platform	Article	Download	Impact	Severity
Windows XP SP3 x86	<a href="#">4500331</a>	<a href="#">Security Update</a>	Remote Code Execution	Critical
Windows XP Professional x64 Edition SP2	<a href="#">4500331</a>	<a href="#">Security Update</a>	Remote Code Execution	Critical
Windows XP Embedded SP3 x86	<a href="#">4500331</a>	<a href="#">Security Update</a>	Remote Code Execution	Critical
Windows Server 2003 SP2 x86	<a href="#">4500331</a>	<a href="#">Security Update</a>	Remote Code Execution	Critical

KPMG MÉXICO DATA BREACH

## Empleados de KPMG descargaron facturas del SAT sin autorización y vulneraron datos personales de sus clientes

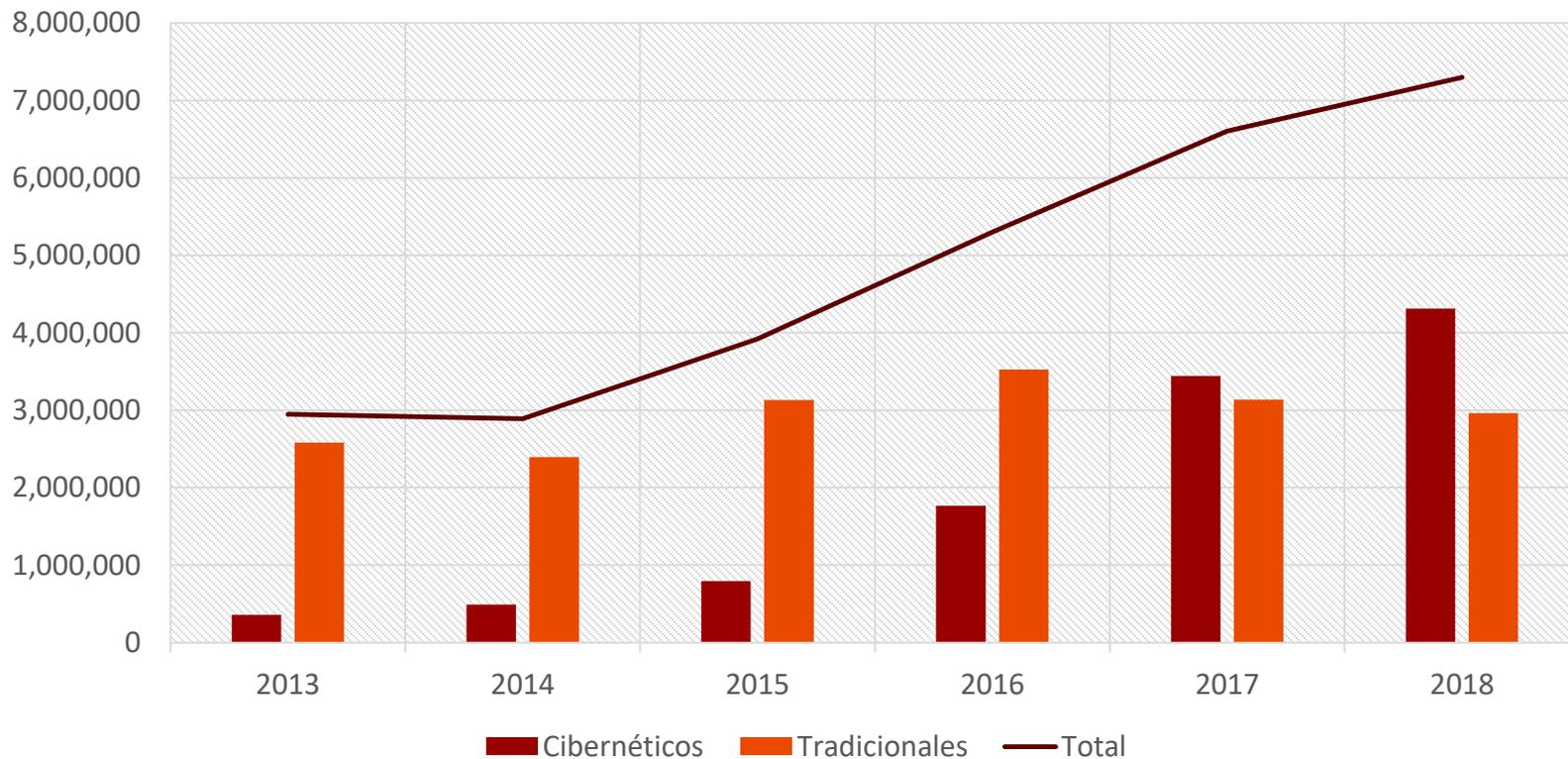


José Soto Galindo

14 de abril de 2019, 15:54



# Reclamaciones por Fraudes



## Monto Reclamado - Fraude Cibernético (MDP) 2018 - \$ 9,517.20

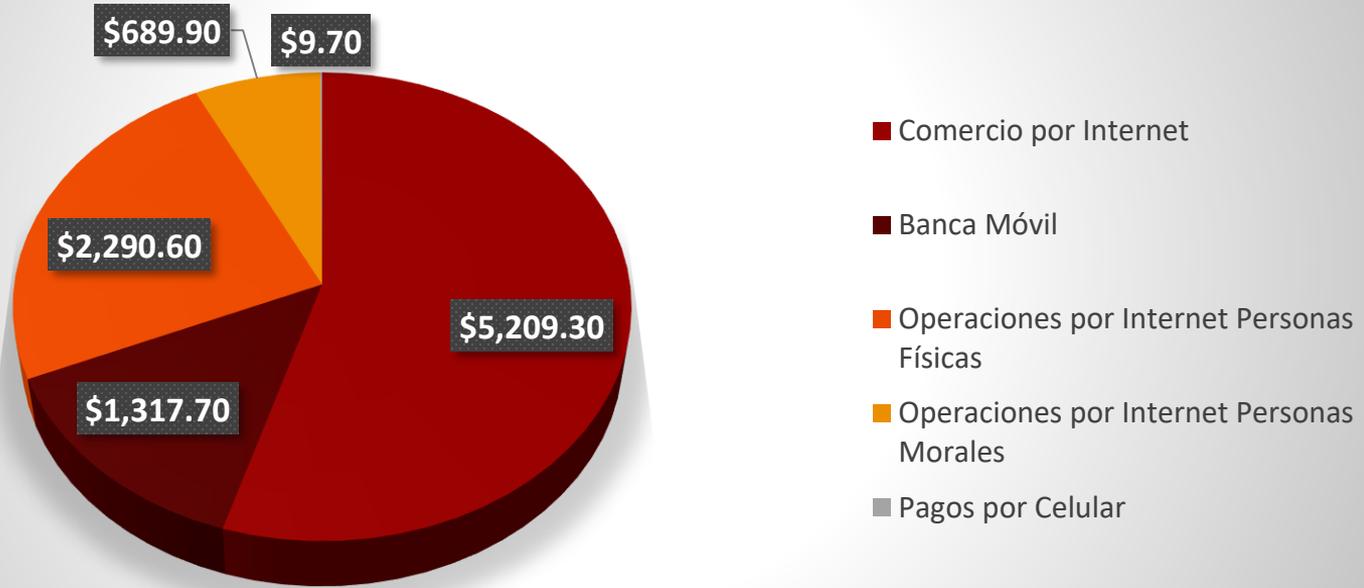


FIGURE 1—RESPONDENT DEMOGRAPHICS

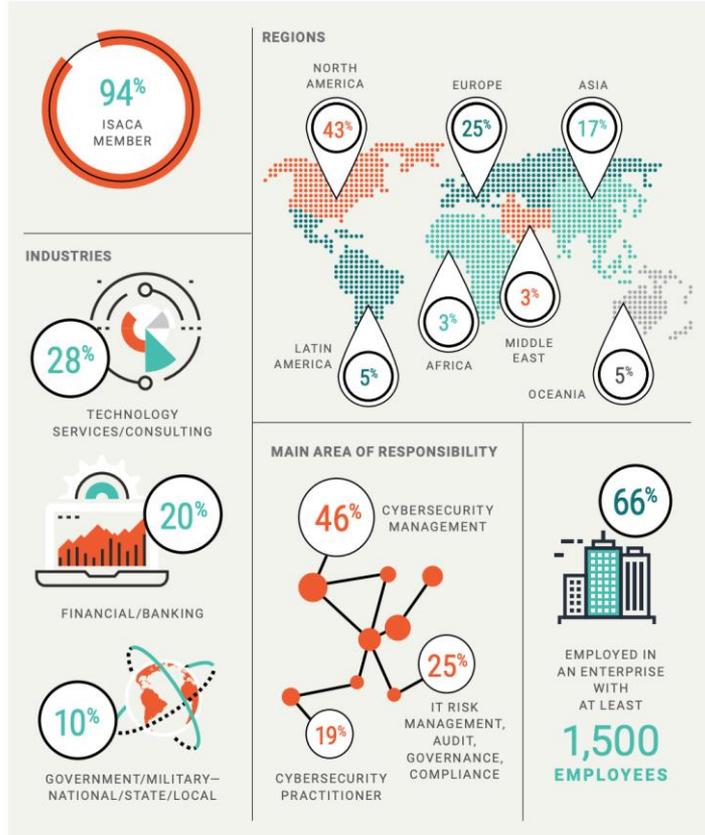


FIGURE 8—BIGGEST SKILL GAP

What is the biggest skill gap you see in today's cybersecurity professionals?

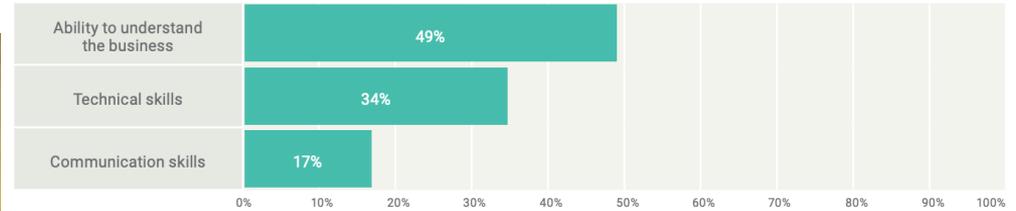
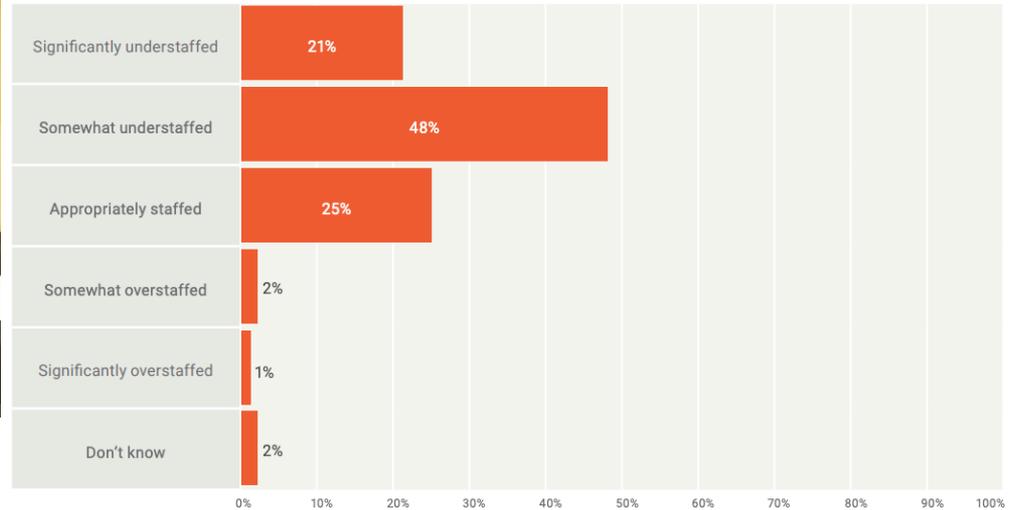


FIGURE 12—PERCEPTION OF CYBERSECURITY STAFFING LEVELS

Do you feel that your organization's cybersecurity team is currently:



REGISTER FOR EXAM

SIGN IN



ABOUT CERTIFICATIONS EDUCATION & TRAINING MEMBERS NEWS & EVENTS ADVOCACY COMMUNITY

Malaysia	324
Malta	18
Martinique	1
Mauritius	22
Mexico	359
Moldova, Republic of	5
Monaco	5
Montenegro	5
Morocco	20
Mozambique	3
Myanmar	3
Namibia	4

131,180 - Mundial

84,557 - US



## Documentos de estrategia nacional de ciberseguridad publicados en 2008-2017 en los países de la OCDE

### Pre-2000

Estados Unidos se ha enfocado en la seguridad cibernética desde los 90s y ha publicado una serie de documentos de ciberseguridad, pero no una estrategia general.

Víctima de un ataque cibernético en 2007, Estonia tiene una de las sociedades más dependientes de la tecnología digital. Hoy en día, la estrategia de ciberseguridad está integrada al proceso de estrategia de defensa nacional

El Reino Unido ha desarrollado una estrategia de seguridad cibernética enfocada a la creación de un entorno seguro para las empresas y el intercambio de información entre sectores (*Fusion Cell*)

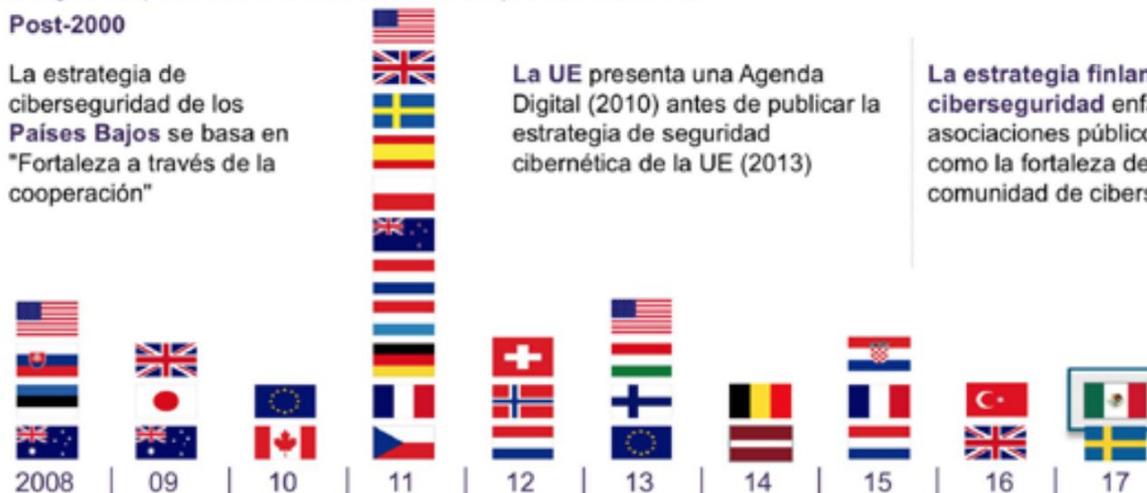
Las estrategias nacionales de ciberseguridad de Francia y Alemania adjudican un papel principal al gobierno

### Post-2000

La estrategia de ciberseguridad de los Países Bajos se basa en "Fortaleza a través de la cooperación"

La UE presenta una Agenda Digital (2010) antes de publicar la estrategia de seguridad cibernética de la UE (2013)

La estrategia finlandesa de ciberseguridad enfatiza las asociaciones público-privadas como la fortaleza de la comunidad de ciberseguridad



### México

2012 – El gobierno de México crea un Comité Especializado en Seguridad de la Información (CESI), encargado de elaborar una Estrategia Nacional de Seguridad de la Información (ENSI)

2017 – El gobierno de México presenta una Estrategia Nacional de Ciberseguridad, desarrollada con el apoyo de la Organización de Estados Americanos (OEA)

FUENTE: Búsqueda web, estrategias nacionales de ciberseguridad



Tabla de Equivalencia Funcional entre Estándares de Seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Seguridad de Datos Personales – Junio 2015



Anexo 28 – Resolución Miscelanea Fiscal – Diciembre 2017  
Seguridad de la Información para Monederos Electrónicos para Combustibles y Vales de Despensa



Disposiciones de Carácter General en Materia de Operaciones de los Sistemas de Ahorro para el Retiro – Noviembre 2018  
De la seguridad de la información, continuidad en la operación y administración del riesgo operativo



Circular Única de Seguros y Fianzas – Septiembre 2016  
Del uso de medios electrónicos para la contratación de operaciones de seguros y de fianzas



Circular Única de Bancos – Noviembre 2018  
De la Seguridad de la Información



Requerimientos en materia de seguridad informática y continuidad operativa a los participantes del SPEI – Mayo 2018



Documento	Institución	Sección de Seguridad de la Información	Tipo																
				SGSI / Programa	Riesgos SI	Prevención	Autenticación	Cifrado	Loggeo	Monitoreo	Continuidad	PenTest / Análisis de Vul.	Revisión General	Privacidad	Clasificación de la Información	Concientización	Incidentes	Actualizado	
Circular Única de Seguros y Fianzas	Comisión Nacional de Seguros y Fianzas	Capítulo 4.10	Regulación		✓	✓	✓	✓				✓					✓		
Disposiciones de Carácter General en Materia de Operaciones de los Sistemas de Ahorro para el Retiro	Comisión Nacional del Sistema de Ahorro para el Retiro	Artículo 90	Regulación		✓			✓				✓	✓					✓	
REGLAS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI)	Banco de México	N/A	Regulación		✓		✓	✓	✓	✓	✓	✓					✓	✓	
Ley Federal de Protección de Datos Personales en Posesión de Particulares	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	N/A	Ley			✓				✓				✓			✓		
Anexo 28 de la Resolución Miscelanea Fiscal	Secretaría de Administración Tributaria	Inciso B y C	Resolución	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Circular Única de Bancos	Comisión Nacional Bancaria y de Valores	Artículo 168 Bis 11	Regulación	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Circular Única para Casas de Bolsa	Comisión Nacional Bancaria y de Valores	Artículo 33	Regulación		✓	✓	✓	✓				✓			✓		✓	✓	
Circular Única de Uniones de Crédito	Comisión Nacional Bancaria y de Valores	Artículo 125	Regulación		✓	✓	✓	✓			✓	✓			✓		✓	✓	



SEGURIDAD DE LA INFORMACIÓN

# Morena propone la creación de una agencia nacional de ciberseguridad

A esta agencia correspondería determinar y coordinar la política estatal en materia de ciberseguridad, así como emitir lineamientos y realizar investigaciones sobre conductas ilícitas realizadas a través de medios informáticos.



Rodrigo Riquelme

02 de abril de 2019, 08:42



**MÉXICO**  
PRESIDENCIA DE LA REPÚBLICA



**2019**  
AÑO DEL CAUDILLO DEL SUR  
EMILIANO ZAPATA

## PLAN NACIONAL DE DESARROLLO

## 2019-2024

# Lo bueno ...

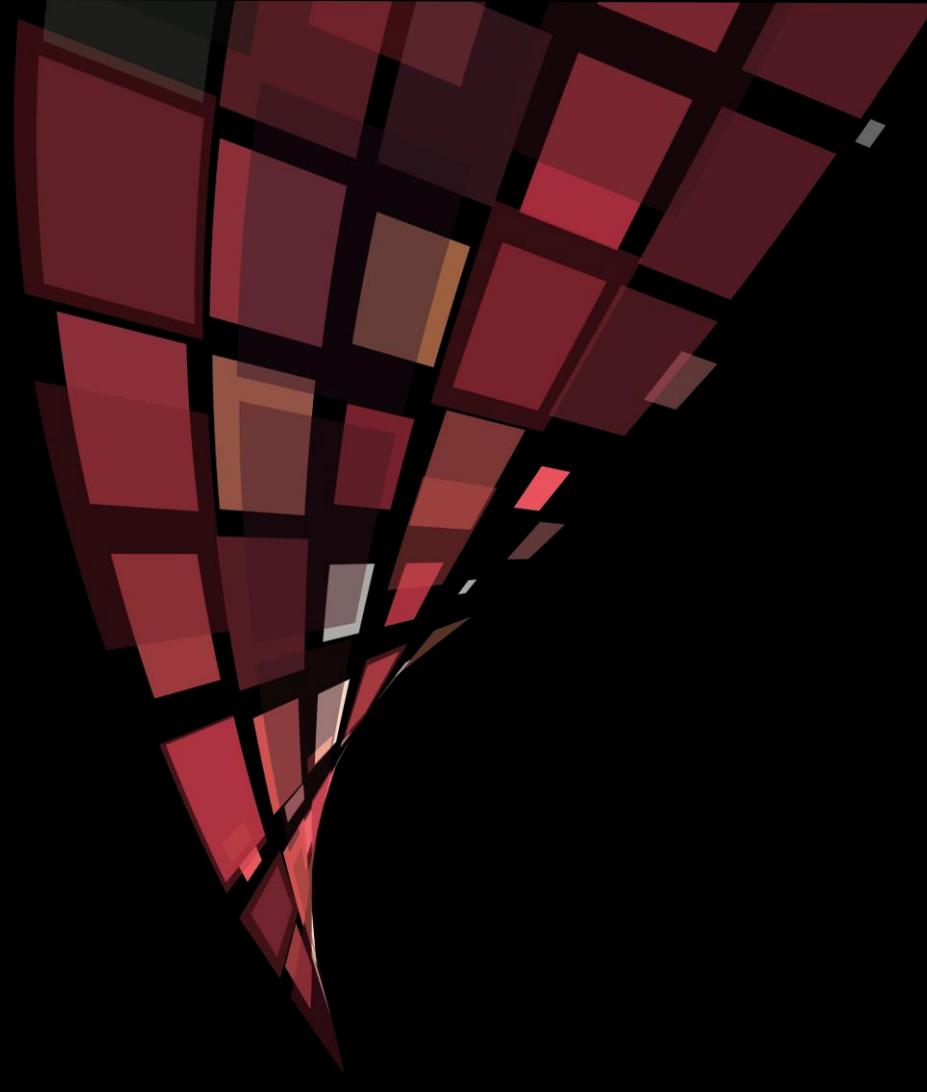
- Interés de la sociedad en general.
- Regulaciones completas (aunque dirigidas).
- Actualizaciones constantes.
- Integración de nuevas regulaciones (Ley Fintech, CoDi).

# Lo malo ...

- Aún estamos un paso atrás del atacante.
- Falta de un Eje Principal (columna vertebral).
- Preocupación solo por cumplimiento.
- Se perdió la continuidad.

# Lo feo ...

- Actualización constante.
- No es prioridad.
- Requerimientos:
  - Tendenciosos (CONSAR).
  - Excesivamente complejos (Anexo 28).
  - No actualizados (CNSF, LFPDPPP).



**CSI** Consultores en  
Seguridad de la  
Información

¡Gracias!

[www.csinfo.com.mx](http://www.csinfo.com.mx)