



## NEWSLETTER – INFOSEC MX

BOLETIN No. 14

MAYO 21-29

Elaboración: Mayo 30,  
2016

### BANCA

**En este número  
encontrarás noticias  
sobre:**

- Banca
- Tecnología
- Salud

## Banca mexicana, sin ciberataques

por MAYO 23 2016 / EL SOL DE MEXICO

El sistema bancario mexicano hasta el momento no ha enfrentado incidentes de ciberataques, afirmó Jorge Palacios, vicepresidente técnico de la Comisión Nacional Bancaria y de Valores (CNBV). En una entrevista, explicó que siempre hay un riesgo tecnológico y operacional en estos sistemas, pero se tiene una de las mejores regulaciones en el mundo. El riesgo operacional se monitorea constantemente, hay reportes mensuales o trimestrales, pero esto no quiere decir que no se haya detectado alguna falla.

México ha estado atento ante las nuevas tecnologías y ha tenido cuidado, un ejemplo es que muchos bancos quieren cambiar su información a la nube, porque es más barato, la Comisión Nacional acepta, pero siempre y cuando el proveedor de la nube cumpla con las condiciones y normas que se exigen para que la comisión pueda auditar esta información, ya que dejó muy claro que si el proveedor de la nube no permitía que se auditaran los datos, entonces no se podía utilizar el servicio, los proveedores han comprendido y aceptado la regulación. Actualmente son pocos los bancos con información en la nube.



Fuente: <http://www.elsoldemexico.com.mx/finanzas/242019-banca-mexicana-sin-ciberataques>

**TECNOLOGÍA**

## Crece velocidad de internet en México

por MAYO 26, 2016 / MILENIO

En México la velocidad del servicio de internet creció un 31.39% en 2015, llegando a 5.8 megabytes por segundo (Mbps) en promedio, quedando como el tercer país con el Internet más rápido en América Latina. Un estudio realizado indicó que a pesar de que falte mucho para llegar al nivel de potencias como Corea del Sur, Suecia o Noruega, México mostró una tendencia positiva durante los últimos dos años; desde que hay un mejor ambiente competitivo que ha empujado a los operadores a realizar más inversiones, mejorar su infraestructura y su oferta de servicios.

El Instituto Federal de Telecomunicaciones (IFETEL), indicó en un informe del cuarto trimestre de 2015, que el 76% de las suscripciones de banda ancha fija en el país navegan a velocidades de entre 10 y 100 Mbps, cinco puntos porcentuales más que en el trimestre inmediato anterior y 64 puntos por arriba del mismo periodo de 2014.

**Fuente:** [http://www.milenio.com/negocios/velocidad-internet-banda\\_ancha-Mexico-Mediatelecom\\_0\\_744525710.html](http://www.milenio.com/negocios/velocidad-internet-banda_ancha-Mexico-Mediatelecom_0_744525710.html)



## Por qué no debes usar contraseñas como "1234"

por MAYO 26, 2016 / MILENIO



Alex Simons, director de la gerencia de programas de Microsoft, publicó en el blog de la compañía que trabajaría para encontrar la manera de mantener la privacidad de sus usuarios mediante un sistema llamado "prohibición dinámica", el cual evita que usuarios de Microsoft utilicen una contraseña muy sencilla o que esté en la lista de las contraseñas más usadas.

Además, esta empresa continuará con su método de bloqueo al intentar varias veces ingresar al sistema, ya que esto evita a los hackers el 54% de las veces, y el 46% restante son usuarios que al olvidar la clave se dan por vencidos.

**Fuente:** [http://www.milenio.com/tendencias/microsoft\\_dynamically\\_banned-contrasenas\\_mas\\_usadas-seguridad\\_internet\\_0\\_744525694.html](http://www.milenio.com/tendencias/microsoft_dynamically_banned-contrasenas_mas_usadas-seguridad_internet_0_744525694.html)

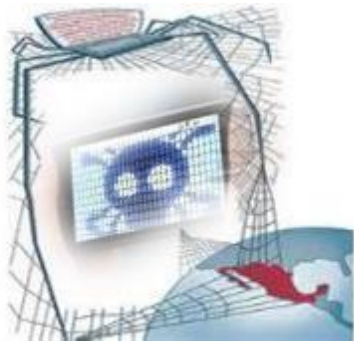
## México, segundo país con más ciberataques a smartphones en América Latina

por MAYO 24, 2016 / PUBLIMETRO

La firma PSafe, indicó que México es el segundo país de Latinoamérica con el mayor número de ciberataques a smartphones, esto debido al desarrollo tecnológico, así como al aumento de transacciones que se realizan por este medio. En el país hay más de 40 millones de smartphones activos, de estos, el 70% usa Android, que es el principal objetivo de los ciberdelicuentes.

Las personas están entre 16 y 17 horas diarias conectadas a Internet con estos dispositivos que gestionan aspectos de sus vidas como datos bancarios, gustos culinarios y de viajes, así como preferencias políticas, por lo que es necesario invertir en Seguridad. Marco De Mello, CEO de PSafe, dijo que un ataque en la vida digital puede ser devastador, las personas pueden tardar hasta dos años en recuperarse y para las empresas puede ser destructivo. Los usuarios no actúan ante los ataques hasta que fueron víctimas de uno.

Fuente: <http://www.publimetro.com.mx/noticias/mexico-segundo-pais-con-mas-ciberataques-a-smartphones-en-al/mpex!xel5MbyZL1ME/>



## Arrumban datos de cédula de identidad de menores

por MAYO 22, 2016 / EXCELSIOR

Francisco Acuña Llamas, comisionado del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai), aseguró que la Secretaría de Gobernación (Segob), tiene una base de datos de 6.8 millones de niños, cuyo uso futuro está en duda, estas fichas de identidad tienen el nombre de los niños, su domicilio, fotografías, imagen del iris y huellas dactilares.

En respuesta, Humberto Roque Villanueva, subsecretario de Población, Migración y Asuntos Religiosos de la Segob, dijo que el banco de datos de la cédula de identidad no corre riesgos y el resguardarla no causa costos adicionales, agregando que el proyecto "está en receso" ya que se quiere integrar los datos biométricos a una clave única de identidad, que será concretada con la modernización de los registros civiles y la depuración de la Clave Única de Registro de Población CURP.

Fuente: <http://www.excelsior.com.mx/nacional/2016/05/22/1094177>



## Facebook cambia normativa interna tras acusaciones de sesgo político

por MAYO 24, 2016 / EL UNIVERSAL

Facebook cambiará las normas internas debido a que fue acusado de ocultar noticias sobre políticos y temas conservadores, acusación hecha por ex empleados de esa red social de manera anónima. Además, no se considerarán las web de medios como la BBC, CNN o "The New York Times" como referentes al evaluar la importancia de las noticias, detalló la empresa en una carta enviada al senador estadounidense John Thune.

Esto generó un debate en medio de la precampaña electoral estadounidense sobre la influencia de Facebook como difusor de noticias. En la investigación llevada a cabo después de las acusaciones, Facebook aseguró no haber detectado un partidismo sistemático. Pero no se puede excluir un comportamiento incorrecto o parcialidad inconsciente de algunos trabajadores, por eso habrá más mecanismos de control y seminarios de formación.

**Fuente:**  
<http://www.eluniversal.com.mx/articulo/techbit/2016/05/24/facebook-k-cambia-normativa-interna-tras-acusaciones-de-sesgo-politico>



## Mexicanos descuidan su privacidad en internet

por MAYO 22, 2016 / EXCELSIOR

Un estudio realizado por Intel Security arrojó que 75% de los mexicanos compartirían información personal como el correo electrónico, un 58% el nombre completo o un 61% la edad en un sitio web, servicio o compañía para un tratamiento para bajar de peso. Destacando que el 8% compartiría su domicilio; 4.0% datos de sus tarjetas de crédito o débito y 6.0% una foto en ropa interior o traje de baño.

El 78% afirmó nunca haber compartido más que una foto normal en línea o vía aplicaciones de texto, correo electrónico o chat. Pero el 15% compartió una imagen en ropa interior o bata de baño con su rostro y el 11% sin mostrar su cabeza. El 6% envió una imagen de su cuerpo desnudo sin su cara y el 2% lo hizo mostrando su rostro. El 59% no sabe cómo comprobar si un sitio web es seguro al proporcionar información personal o detalles de pago. Además, 7 de cada 10 usuarios de Internet hacen clic en ventanas emergentes de promociones y dietas sabiendo los peligros informáticos que implica esto.

**Fuente:** <http://www.excelsior.com.mx/hacker/2016/05/22/1094224>



## La forma en que los mexicanos navegan en la red

por MAYO 17, 2016 / EXCELSIOR

Según Nielsen IBOPE, en México más del 60% hace uso del Internet por lo menos una vez al mes, esto debido a una mayor cantidad de dispositivos para conectarse. Según datos de TGI, el 49% de personas se conectan a través de smartphones, 40% en computadoras, 31 % en laptops y 9% por tabletas. Los SmartTVs y consolas de videojuegos son usadas por el 1%. Las páginas más visitadas son Google, con 93%; Youtube con 58%. El 26% buscan en Internet productos anunciados al ver la televisión (conocido como Meshing).

El acceso a Internet se da en su mayoría entre semana, esto entre las 18:00 y las 20:00 horas con un 45%, un porcentaje igual entre las 20:00 y las 22:00 horas. Entre las 15:00 y las 18:00 horas, con un 37%. El 80% se conecta en su casa, un 15% en el trabajo y un 8% en cibercafés. Un 85% envía mensajes instantáneos, el 70% envía mensajes por medio de WhatsApp, y el 69% usa el Facebook Messenger. En Facebook y Twitter un 84% se conecta a estas plataformas, un 53.5% lo hace para publicar contenidos u opiniones.

Fuente: <http://www.excelsior.com.mx/hacker/2016/05/17/1093297>



## México, el quinto país más atacado en el mundo cibernético: Fortinet

por MAYO 17, 2016 / EXPANSION

En menos de tres meses, México pasó del séptimo lugar al quinto, esto a nivel mundial, indica la compañía Fortinet, estando Estados Unidos, Japón, Alemania y Canadá antes. Los virus que más atacan en México son: JS, Cryptwall, Word Macro y Excel Macro. Además, se encuentra en tercer lugar en Botnets, detrás de EU y Japón.

En el mundo, Fortinet detecta 50,000 millones de intentos de ataques a redes y equipos cada día. Esta industria que incluye hackeo, lavado de dinero, secuestro de equipos, entre otros delitos, tiene un valor aproximado de un billón de dólares. Entre el primer trimestre de 2015 y el mismo periodo de 2016, el número de ataques con malware tuvo un crecimiento de 1,351%. Así mismo, se reportan cada vez más ataques a dispositivos móviles, siendo el crecimiento interanual del 661%.

Fuente: <http://expansion.mx/tecnologia/2016/05/26/mexico-el-quinto-pais-mas-atacado-en-el-mundo-cibernetico-fortinet>



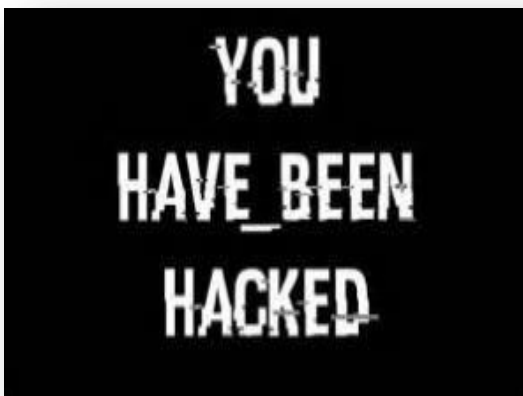
## Have I been pwned? La web que te permite comprobar si tu cuenta ha sido hackeada

por MAYO 24, 2016 / CCM

El investigador Troy Hunt, tiene una web llamada "Have I Been Pwned?", donde recopila los datos de las brechas de Seguridad, la cual sirve para comprobar si ha sido víctima de algún hackeo masivo. Ha conseguido acceso a una copia de los datos robados de LinkedIn y ha actualizado la página.

Esta web cuenta con un buscador que vemos nada más acceder a la misma, donde podemos introducir nuestro correo electrónico o nombre de usuario, buscará entre todos los datos recopilados en los últimos tiempos y devolverá un informe detallado. Cuenta actualmente con una base de datos que incluye las credenciales de 106 páginas webs y 510 millones de cuentas hackeadas. También informa si nuestra cuenta forma parte de una "Sensitive breach", una brecha que no se hace pública por razones de Seguridad.

Fuente: <http://es.ccm.net/news/20161-como-saber-si-tu-cuenta-ha-sido-hackeada>



## Las nuevas amenazas de Seguridad, los retos para el 2016

por MAYO 19, 2016 / NETMEDIA

Norton by Symantec, elaboró un listado con las 10 tendencias en Seguridad que han marcado estos primeros meses del año, apuntando que diariamente se detectan un millón de ataques a sitios web, y el phishing registró un aumento de 55% y el 75% de las páginas de internet son inseguras. Estas son las 10 tendencias que transformarán los objetivos en materia de ciberseguridad durante el resto de 2016:

- Vulnerabilidades "Día Cero"
- Robo y pérdida de identidad: la mega filtración
- Smartphone y sistemas Mac son objeto de ataques Herramientas más sofisticadas
- El Internet de las Cosas también es el internet de las vulnerabilidades
- Sitios web legítimos pueden no ser lo que aparentan
- Los estafadores técnicamente ya no son los mismos
- Usuarios de Apple están cada vez en mayor riesgo
- Los riesgos en redes sociales te harán pensar dos veces antes de dar un "like" y por último:
- El secuestro de dispositivos está en aumento.

Fuente: [http://www.netmedia.mx/b-secure/las-nuevas-amenazas-de-seguridad-los-retos-para-el-2016/?utm\\_content=buffer951c4&utm\\_medium=social&utm\\_source=twitter.com&utm\\_campaign=buffer](http://www.netmedia.mx/b-secure/las-nuevas-amenazas-de-seguridad-los-retos-para-el-2016/?utm_content=buffer951c4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer)

## 6 de cada 10 consumidores demandarían a las compañías que gestionan datos si se produce un robo

por MAYO 19, 2016 / SILICON

Josh Goldfarb, CTO de Emerging Technologies de FireEye, señala que después de una sustracción de datos, aunque las organizaciones intenten recuperar la confianza de sus clientes con compensaciones, estos daños tanto económicos como la pérdida de reputación, permanece por mucho tiempo después del incidente.

Agregó que el 70% comparte menos datos con las empresas por los últimos incidentes de Seguridad, aún sin tener nada que ver con la compañía con la que ellos se relacionan, limitando la capacidad de las empresas para ofrecer productos y servicios personalizados y adaptados. El 73% de los consumidores, cancelaría servicios al enterarse que sus datos han sido sustraídos por un problema de Seguridad. Un 25% considera que su información corre riesgo con compañías que ya han sufrido algún ataque. El 50% pagaría más por un servicio o producto más seguro. Y el 60% iniciaría medidas legales contra una compañía si sus datos acaban en manos de terceros y usados para delinquir.

**Fuente:** [http://www.silicon.es/6-de-cada-10-consumidores-dispuestos-a-demandar-a-companias-que-gestionan-datos-si-se-produce-un-robo-2308901?utm\\_content=buffer9e7e3&utm\\_medium=social&utm\\_source=twitter.com&utm\\_campaign=buffer#FLDZ3UJhbEz3qQls.99](http://www.silicon.es/6-de-cada-10-consumidores-dispuestos-a-demandar-a-companias-que-gestionan-datos-si-se-produce-un-robo-2308901?utm_content=buffer9e7e3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#FLDZ3UJhbEz3qQls.99)



## 52% de empresas mexicanas usan softphone pirata

por MAYO 26, 2016 / FORBES



Según una investigación global realizada por la firma BSA, The Software Alliance, el 52% de las empresas mexicanas usan software pirata, y el uso del mismo crece de manera alarmante, sin embargo, en México, el porcentaje del software ilegal instalado bajó un 2%. El costo por usar software malicioso para las empresas fue de 400,000 millones de pesos en ciberataques.

El uso de software pirata llegó a una tasa global de 25% para las empresas en el sector bancario, de seguros y de valores. Además, el 60% de los empleados en empresas tecnológicas reconoció el riesgo de Seguridad relacionado con el software sin licencia.

**Fuente:** <http://www.forbes.com.mx/52-de-empresas-mexicanas-usan-software-pirata/>

**SALUD**

## Por robo de identidad, suman 561 denuncias en ZMG

por MAYO 18, 2016 / PROYECTO DIEZ

Un total de 561 denuncias por este delito fueron presentadas en la Zona Metropolitana de Guadalajara (ZMG) de enero a marzo de este año. En Guadalajara se registraron más con 375 denuncias, según Ignacio Vázquez, ingeniero en Seguridad electrónica y redes, publicar datos reales y completos en las redes sociales es un error, ya que facilita el robo de identidad.

Con el nombre completo y la fecha de nacimiento (día, mes y año), un criminal podría conseguir datos personales como son la Clave Única de Registro de Población (CURP), el número de seguro social o el Registro Federal del Contribuyente (RFC).

Fuente: <http://www.proyectodiez.mx/suman-561-denuncias-por-robo-de-identidad-en-lo-que-va-del-ano-en-la-zmg/>



## Sector salud, el nuevo blanco del ransomware

por MAYO 23, 2016 / ITSITIO

En hospitales los equipos de las diferentes áreas están interconectados compartiendo datos de pacientes, rayos X y tomografías computarizadas, estos sistemas seguido no son segmentados en distintas redes o zonas de Seguridad, por lo que cuando los datos son cifrados por ransomware las operaciones diarias se paralizan por completo porque algunas partes de la cadena ya no están disponibles.

No todos los hospitales tienen los recursos para que personal de Seguridad informática esté de lleno dando Seguridad a la Información y a monitorear la red. La prioridad es mantener los sistemas disponibles todo el tiempo; aunque algunos de los principios básicos de Seguridad en la arquitectura de red y la protección de datos confidenciales (incluyendo copias de Seguridad) deben estar siempre implementados. Un ejemplo es no permitir que dispositivos médicos con sistema operativo obsoleto se conecten a Internet, permaneciendo en una zona de red segmentada y separada para un departamento del hospital y con reglas de acceso que regulen su conexión entre esas zonas.

Fuente: <http://usa.itsitio.com/sector-salud-el-nuevo-blanco-del-ransomware/>







# TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 14

MAYO 21-29, 2016

Elaboración: MAYO 30, 2016

**totalsec**  
Security Operation Center