



CDMX
CIUDAD DE MÉXICO



INFORMACIÓN GENERAL

Ofertan en internet las TVs del Apagón Analógico

Vende empresa teles 'regaladas'

Compañía Synnex oculta la leyenda 'Mover México' en dichos equipos

JUAN MANUEL GONZÁLEZ

Una de las empresas que participó en el reparto gratuito de televisores digitales para familias de escasos recursos en 2015 ahora vende el mismo modelo que entregó, pero con la leyenda "Mover México" oculta.

La empresa Synnex de México hace negocio con los receptores a los cuales sobrepuso una placa metálica de la marca Fuze para ocultar el eslogan de la actual Administración "Mover México" y que era el sello característico de los aparatos que el Gobierno federal repartió.

REFORMA adquirió el pasado 11 de enero un televisor ofertado bajo la descripción "Televisión FUZE, Pantalla LED 23.6" HD Negra". La solicitud se hizo vía electrónica.

Al recibir el paquete pudo comprobarse que el equipo tiene una placa sobrepuesta en emblemas gubernamentales y no tiene ninguna advertencia de que se trate de pantallas destinadas para un uso oficial.

Este tipo de televisiones puede adquirirse en compras electrónicas desde el pasado

Mueven... la leyenda

Los equipos, ofertados en internet, lucen una etiqueta con la marca Fuze, que, al ser removida, dejan ver la leyenda "Mover México"

Televisión FUZE, Pantalla LED 23.6" HD Negra

Precio recomendado: \$2,990.00

Precio: \$2,199.00 Envío GRATIS. Detalles
Ahorras: \$791.00 (26%)



Francisco Barrón

14 de junio de 2017. De ese día a la fecha su precio ha fluctuado entre los mil 649 y los 2 mil 199 pesos, costo al que se comercializa actualmente.

Según los registros de Amazon, el viernes 12 de enero ocupó el cuarto lugar de los televisores más comprados en el sitio.

La empresa Synnex de México, con sede en Azcapotzalco, obtuvo el 26 de noviembre de 2015 vía adjudicación directa número SA-009000987-N88-2015 un contrato con la SCT para entregarle 250 mil televisores

digitales por un monto de 577 millones de pesos.

Un año después, el 28 de septiembre de 2016, giró un oficio a la dependencia federal para manifestar que había cumplido el contrato al entregar el total de los televisores convenidos.

Según se desprende de su sitio web, sus clientes son primordialmente entes de Gobierno.

El programa de transición digital y entrega gratuita de televisores ha estado en el ojo del huracán. El Gobierno regaló más de 10 millones de aparatos adquiridos a varias

empresas, entre ellas Synnex.

En 2016, Adolfo Cuevas, comisionado del Instituto Federal de Telecomunicaciones (IFT) consideró que 54.83 por ciento del total de televisiones se distribuyeron en hogares que no lo necesitaban, lo que representó un derroche de 16 mil millones de pesos.

Pero la Auditoría Superior de la Federación (ASF) fue más allá. En julio de 2017 señaló que la SCT reportó la pérdida de 11 mil 533 televisores y estimó un posible daño patrimonial de 29.2 millones de pesos.

PGR, lista para contener ciberataques electorales

- Ofrece ayuda al INE para blindar sus sistemas informáticos
- Destaca la importancia de prevenir y tener protocolos de reacción

ELECCIONES 2018

MANUEL ESPINO

—justiciaysociedad@eluniversal.com.mx

La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Procuraduría General de la República (PGR) se reporta lista para apoyar al Instituto Nacional Electoral (INE), si así lo desea, en el blindaje de sus sistemas informáticos que pueden ser blanco de grupos hacktivistas o hackers durante el proceso electoral de este año.

Marcos Rosales García, titular de esa área adscrita a la Agencia de Investigación Criminal, reconoce que el INE cuenta con un sistema de avanzada, que les permite tomar medidas para mantenerse libre de ataques cibernéticos, “pero si requieren apoyo ahí estaremos”.

En entrevista con EL UNIVERSAL, explicó que los ataques cibernéticos que se han detectado van dirigidos en diferentes sentidos: el robo de información de los equipos y los que buscan afectar la infraestructura para dejarla fuera de línea. Entre ellos están “los grupos hacktivistas”, que tienen fines políticos.

El funcionario presume que, a cuatro meses de su creación, la unidad identificó y mitigó más de 289 incidentes de seguridad informática que afectaban tanto al sector público como al privado, entre ellos la erradicación del virus *FALLCHILL*, de origen norcoreano, en una operación conjunta con el FBI.

“Al estar interconectados, todos

“Si el INE nos requiere para buscar proteger alguna de sus infraestructuras, por supuesto que lo haríamos”

MARCOS ROSALES GARCÍA

Titular de Investigaciones Cibernéticas

los riesgos que ocurran alrededor del mundo son riesgos que eventualmente podemos recibir en nuestro país, pero ayuda alertar sobre mecanismos de prevención y, en caso de no poder prevenir, tener los protocolos de reacción”, dijo.

NACIÓN A14



LUIS CORTÉS, EL UNIVERSAL

Para el jefe de la Unidad de Investigaciones Cibernéticas, hay que estar reinventando los protocolos, porque las actividades criminales evolucionan.



Marcos Rosales García

Titular de la Unidad de Investigaciones
Cibernéticas y Operaciones Tecnológicas
de la PGR

“Podemos blindar al INE contra hackers”

- De ser requeridos, se ayudará a proteger sistemas electorales, dice
- Asegura que México es posible objetivo de algunos ciberataques

ELECCIONES 2018

MANUEL ESPINO

—justiciaysociedad@eluniversal.com.mx

La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT) de la PGR se creó en septiembre del año pasado y su titular, Marcos Rosales García, asegura que a pesar del poco tiempo en operación, están listos para apoyar al Instituto Nacional Electoral (INE), si así lo desea, en el blindaje de sus sistemas informáticos, que pueden ser blanco de grupos hacktivistas o hackers durante el proceso electoral.

En entrevista con EL UNIVERSAL, reconoce que el INE cuenta con un sistema de avanzada. Rosales García afirma que en esta materia no hay nada que sea 100% seguro, por lo que "si el INE nos requiere para proteger alguna de sus infraestructuras, por supuesto que lo haríamos".

ENTREVISTA

Presume que en el último cuatrimestre de 2017, la Unidad de Investigaciones identificó y mitigó más de 289 incidentes de seguridad informática que afectaban tanto al sector público como privado.

En la sede de la Agencia de Investigación Criminal, el funcionario destaca la erradicación del virus informático denominado *FALLCHILL*, de origen norcoreano, en una operación conjunta con el FBI, como el principal logro de la unidad, con apenas cuatro meses de creada.

Su objetivo, expone, era "robar información que estaba almacenada en los equipos de cómputo. Muchas veces buscan la información financiera que les permita hacerse de algunos recursos. Si se hubiera instalado en una infraestructura sensible, en la que la información que se almacena es de carácter confidencial o sensible, pues es explotable para los grupos que desarrollan estos malware".

Recuerda que al "estar interconectados con todo el mundo, todos los riesgos que ocurran alrededor del mundo son riesgos que eventualmente podemos recibir en nuestro país, pero estar alertando sobre cuáles son los mecanismos de prevención, ayuda". Ante ello, reveló que está en marcha un operativo conjunto con Interpol por amenazas de posibles ataques contra la infraestructura tecnológica del país.

¿Cuál es la incidencia de delitos cibernéticos en México?

—Hemos operado diferentes acciones en contra del cibercrimen, realizamos un par de operativos coordinados por Interpol, en los que muchos países alrededor del mundo, particularmente de América Latina, hemos participado y obtenido resul-

tados importantes en la desarticulación de grupos cibercriminales.

Es importante decir que en nuestro país no tenemos estadística relacionada con los delitos cibernéticos que nos permita medir cuál es el impacto real que tienen estas conductas en contra del ciberespacio mexicano y particularmente los usuarios que están en la red nacional.

¿Cuáles son los delitos que más cometen los cibercriminales y que detecta la UICOT?

—Hemos tenido muchos casos de clonación de sitios oficiales por parte de grupos hacktivistas o de hackers, que buscan robar información de una persona o generar algún tipo de estafa creando páginas apócrifas.

Es el delito más común, pero también hay ataques por denegación de servicio distribuido. Esto último quiere decir que muchos equipos hacen solicitudes a un solo servidor y eventualmente queda fuera de línea. Hay una gran variedad de delitos y algunos, por las temporadas, pueden ser más recurrentes que otros.

¿Cuáles delitos aumentan y en qué temporada?

—Cuando hay muchas compras en línea, los fraudes al comercio electrónico aumentan.

¿Cuántos ataques cibernéticos han detectado?

—Los ataques cibernéticos dirigidos van en diferentes sentidos: el robo de información de los equipos y los que buscan afectar la infraestructura para dejarla fuera de línea.

Así también hemos tenido ataques a sitios gubernamentales, a empresas. Particularmente, el malware que recientemente identificamos y que logramos desactivar estaba alojado en una empresa de telecomunicaciones, entonces no es un tema exclusivo de las dependencias gubernamentales.

Si bien muchas veces pueden ser objetivos con fines políticos, hay otros que lo que buscan es hacerse llegar de algún recurso y lo obtienen de empresas privadas, no del gobierno.

¿Han detectado ataques de grupos de hacktivistas?

—Sí, por supuesto. En algunos de los operativos que hemos participado anteriormente, hemos logrado identificar a, por lo menos, un par de grupos hacktivistas, uno con origen en Perú y otro en África. Hemos dado parte a las autoridades de estos países y les hemos entregado toda la información que hemos podido recolectar, para que ellos a su vez continúen con las líneas de investigación que puedan sancionar todas estas conductas.

¿Cómo detectaron el virus informático de origen norcoreano?

—El Homeland Security Investigations y el FBI identificaron el año pasado que estaba circulando por la red un código malicioso, realizaron una

“Hemos tenido muchos casos de clonación de sitios oficiales por parte de grupos hacktivistas o de hackers”

“Tuvimos un operativo con Interpol, en el que nos están dando información sobre posibles ataques en contra de la infraestructura de nuestro país”

investigación técnica con los datos que obtuvieron y definieron que un virus realizaba actividades como la de instalarse en un equipo de cómputo.

Definieron un análisis técnico e identificaron que se distribuía en diferentes países y ubican que la información que se filtraba de los equipos que ya habían sido víctimas, se dirigía a una red con origen en Corea del Norte, por eso es que logran determinar el origen de estos códigos maliciosos.

El FBI dio parte a la PGR de que este virus podría estar en la red nacional, por lo que la unidad se puso a investigar y logró identificar que existían algunos servidores que habían sido comprometidos y nos pusimos en contacto con la empresa para hacerle saber la situación que tenía y tomar las medidas para que el virus no se siguiera propagando.

¿Cuál era la intención de ese malware en los equipos?

—Robar información que estaba almacenada en los equipos de cómputo, pero muchas veces buscan información financiera que les permita hacerse de algunos recursos. Si se hubiera instalado en una infraestructura sensible, donde la información que se almacena es de carácter confidencial o sensible, pues es explotable para estos grupos hacktivistas o para los que desarrollan estos malware.

¿Los sistemas informáticos del gobierno y de las instalaciones estratégicas están blindados?

—No hay nada que sea 100% seguro, esa es una máxima, lo cierto es que el gobierno federal ha venido trabajando, desde hace algunos años, en cómo proteger todo el ciberespacio mexicano. El año pasado se presentó la estrategia nacional de ciberseguridad, un parteaguas.

¿La UICOT protege la red informática del gobierno federal?

—Hoy, diferentes dependencias están participando para garantizar un internet seguro en nuestro país. Es importante señalar que no existe una barrera física para aislar el internet mexicano del mundial, al estar interconectados con todos los países, todos los riesgos que ocurran alrededor del mundo son riesgos que, eventualmente, podemos recibir en nuestro país, pero el siempre estar emitiendo boletines de cuáles son los mejores mecanismos de prevención, ayuda y, en caso de que no podamos prevenir, tener los protocolos de reacción para mitigar aquellos riesgos que se estén explotando y que una vulnerabilidad, haya sido explotada y que no tengamos una afectación.

Últimamente se ha mencionado una posible intromisión del exterior en el proceso electoral. ¿Ustedes podrían brindar apoyo técnico al INE para blindar su sistema y evitar que el instituto sea víctima de un ataque cibernético?

—Por supuesto que sí. Una de las líneas de acción de esta unidad es la protección de información y buscar la ciberseguridad de las diferentes dependencias, organismos y empresas.

Si el Instituto Nacional Electoral nos requiere para buscar proteger alguna de sus infraestructuras, por supuesto que lo haríamos.

Nosotros hacemos diferentes cosas, una de ellas es estar monitoreando la red pública de internet a través de lo que nosotros estamos buscando, que es la comisión de delitos en internet, como la venta de droga, de armas, de artículos sin tener los derechos de autor.

¿Cuentan con la tecnología necesaria para apoyar al INE?

—Eso dependería de qué es en lo que ellos quieren que los apoyemos, la infraestructura tecnológica del INE es amplia y tienen un área de ciberseguridad que ha venido trabajando de manera adecuada a lo largo de los años. Tienen un Comité de Ciberseguridad que les permite tomar medidas para mantenerse libres de los ataques cibernéticos, pero si en algún momento requieren apoyo, ahí estaremos.

¿Han detectado riesgos de ataques cibernéticos?

—Hemos estado trabajando de manera coordinada con diferentes agencias alrededor del mundo. Recientemente tuvimos un operativo con Interpol, de hecho continúa, en el que nos están dando información sobre algunos posibles ataques en contra de la infraestructura de nuestro país.

Nosotros validamos que realmente está ocurriendo esa situación, levantar un protocolo para poder mitigar ese riesgo y poner en operación la plataforma que haya sido afectada.

La UICOT es de reciente creación y tenemos que ir avanzando a un nivel de maduración tal, que nos permita tener un grado de operación óptimo para poder brindar todas las capacidades que requiere el ciudadano en materia de prevención y persecución de los delitos cibernéticos.

¿Se han visto vulneradas las instalaciones estratégicas del país?

No tenemos ningún caso documentado, como país, donde alguna instalación o alguna infraestructura crítica haya sido afectada de manera grave, no tenemos ningún caso en el país afortunadamente.

Creo que los protocolos que se han implementado para prevención y afectación de infraestructuras sensibles han funcionado adecuadamente, pero hay que estar reinventando estos protocolos, porque las actividades criminales evolucionan. ●



www.eluniversal.com.mx

Vea el video



EVITARON ALZA ABRUPTA

70 mil mdp amortiguaron gasolinazo

En 2017, la Secretaría de Hacienda sólo recaudó 75% del IEPS proyectado en la Ley de Ingresos; ésta fue la estrategia para "suavizar" precios de combustibles

POR PAULO CANTILLO

La política de estímulos al Impuesto Especial sobre Producción y Servicios (IEPS) aplicada en 2017 a los precios de los combustibles generó una pérdida por 70 mil millones de pesos en recaudación al gobierno federal, lo que representa 25% de lo proyectado para ese gravamen.

Al inicio del año pasado, se contemplaba una recaudación del impuesto por 284.5 mil millones de pesos. Sin embargo, los cálculos de la Secretaría de

Hacienda y Crédito Público indican que al cierre del año se habrían recaudado 214.5 mil millones de pesos (75%).

Lo que se dejó de recaudar equivale al presupuesto de un año del Seguro Popular, el Poder Judicial, de la Secretaría de Agricultura o la Secretaría de la Defensa Nacional.

Adrián García, investigador en Ingresos Tributarios del Centro de Investigación Económica y Presupuestaria (CIEP), explicó que los estímulos al IEPS pretendieron evitar un costo político al gobierno

por una alza abrupta en los precios de las gasolinas.

Agregó que este año "también se observará una pérdida

recaudatoria porque el precio del petróleo está por encima de los 48.5 dólares por barril".

DINERO | PÁGINA 6

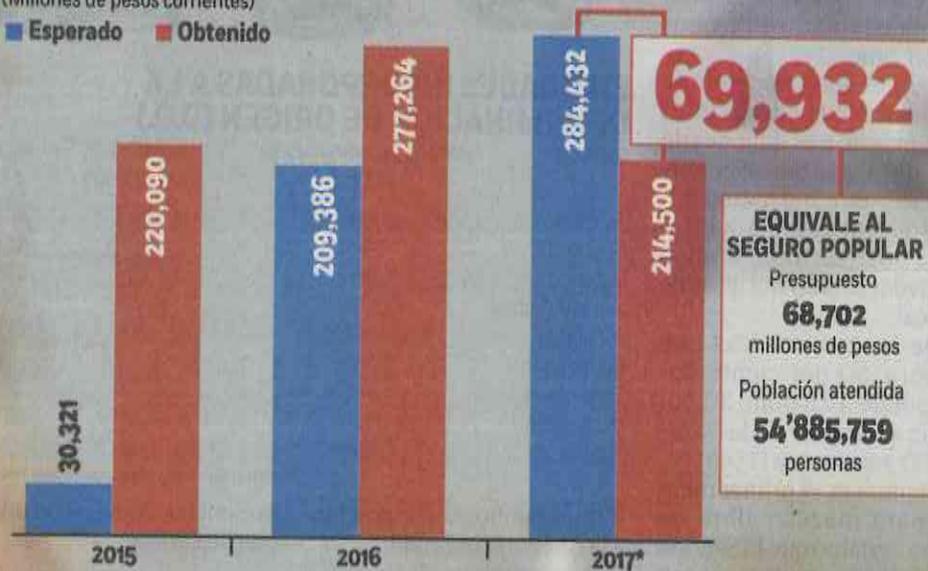
COSTOSO, CONTENER GASOLINAZO

La pérdida recaudatoria por otorgar estímulos al IEPS de gasolinas para evitar alzas abruptas en los precios al público fue por 70 mil millones de pesos >6

RECAUDACIÓN EN LOS COMBUSTIBLES

(Millones de pesos corrientes)

Esperado Obtenido



* Lo obtenido corresponde a la estimación de la Secretaría de Hacienda.

EL CASO DE LA MAGNA: SUBSIDIO A AUTOMOVILISTAS

(Pesos por litro)

Autorizado Cobrado



Fuente: Excelsior, con datos de la SHCP y Gesoc.

SECRETARÍA DE HACIENDA

Subsidiar gasolina costó 70 mil mdp

Con esta estrategia se evitó que los precios al público se elevaran después del gasolinazo del mes de enero

POR PAULO CANTILLO
paulo.cantillo@gmm.com.mx

El gobierno habrá incurrido en una pérdida recaudatoria de 70 mil millones de pesos debido a la política de estímulos al Impuesto Especial sobre Producción y Servicios (IEPS) aplicado a gasolinas y diesel durante 2017, con el fin de evitar que los precios al público se elevaran después del gasolinazo de enero, según cálculos de la Secretaría de Hacienda.

Así, la Ley de Ingresos del año pasado consideraba una recaudación total del impuesto por 284.5 mil millones de pesos, pero Hacienda proyectó que al cierre de 2017 se habrán recaudado 214.5 mil millones de pesos.

La pérdida recaudatoria es equivalente al presupuesto del Seguro Popular, el Poder Judicial, de la Secretaría de Agricultura o la Secretaría de la Defensa Nacional.

De acuerdo con la Ley del IEPS, el gobierno tenía autorizado cobrar 4.30 pesos por litro en la gasolina Magna, 3.64 pesos por litro en la Premium y 4.73 pesos por litro de diesel; sin embargo, la meta de recaudación no se alcanzará debido a que el gobierno nunca cobró el tope posible para la Magna y el diesel, y en la Premium sólo lo cobró en al-

gunas semanas.

La estrategia de "suavización de precios" consistió en que, cuando éstos, a nivel internacional, y el tipo de cambio presionaban los precios locales, el gobierno daba un estímulo con lo que cobraba menos IEPS en los combustibles; mientras que, cuando la cotización global y el dólar bajaban, había margen de reducir los estímulos y con ello cobrar más impuestos.

FACTORES

Adrián García, investigador en Ingresos Tributarios del Centro de Investigación Económica y Presupuestaria (CIEP), explicó a **Excelsior** que los estímulos semanales al IEPS de combustibles pretenden evitar un costo político al gobierno para que los precios no aumenten abruptamente, y más en un contexto electoral.

Añadió que "este año también se observará una pérdida recaudatoria debido a que el precio del petróleo está por encima de los 48.5 dólares por barril aprobado para el Presupuesto 2018. En la medida en que el precio del crudo aumente, el gobierno se verá obligado a otorgar más estímulos al IEPS para evitar alzas en las gasolinas."

De acuerdo con el experto, los estímulos seguirán otorgándose en el corto y

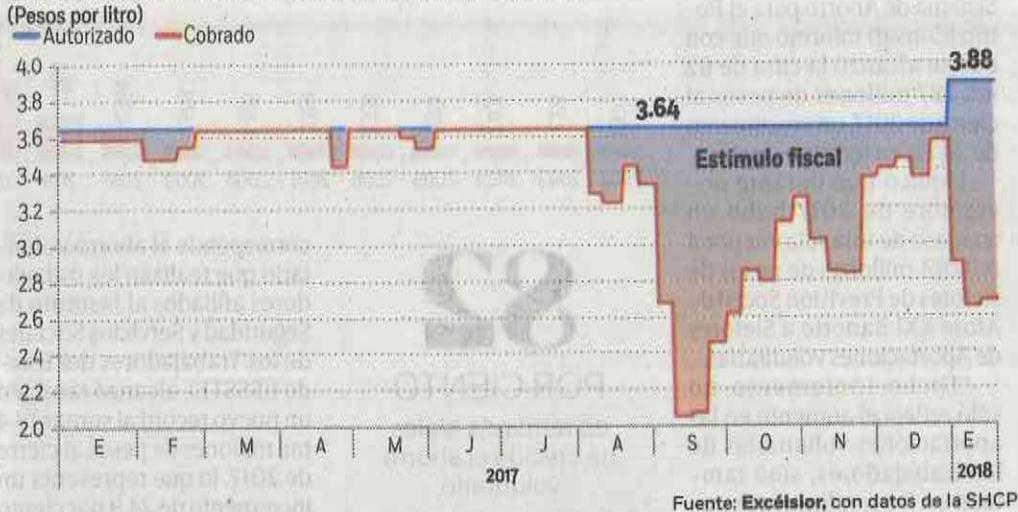
mediano plazos, puesto que, además del criterio político, "el gobierno también tratará que las gasolinas no impacten más la inflación, como sucedió el año pasado".

ESCENARIO IDEAL

García manifestó que en el mediano y largo plazo, "lo ideal" es que el gobierno establezca un IEPS de gasolinas fijo para todo el año y que el precio fluctúe conforme a las condiciones de mercado.

"Con ello se garantiza una recaudación relativamente estable".

EN EL CASO DE LA GASOLINA PREMIUM



Fuente: Excelsior, con datos de la SHCP

Estímulos alcanzan el 50%

El gobierno federal habrá otorgado un estímulo fiscal cercano al 50% sobre la cuota del IEPS en la gasolina Magna durante los primeros 19 días de enero, de acuerdo con datos de la Secretaría de Hacienda y Crédito Público.

Así, de los 4.59 pesos que la ley del IEPS faculta al gobierno a cobrar por cada litro del combustible, del 1 al 5 de enero se cobraron 2.254 pesos; del 6 al 12 se hizo en 2.254 pesos, y del 13 al 19 del mes se cobrarán 2.339 pesos.

Para el caso de la gasolina Premium, de los 3.88 pesos establecidos en la ley del IEPS, se ha otor-

gado en promedio 29.51% por estímulos; y para el diesel, de los 5.04 pesos autorizados, se han dado al público subsidios por 55.54% del valor en promedio en el mismo lapso.

Según lo establecido en la Ley del IEPS y el Código Fiscal de la Federación, las cuotas máximas a cobrar por IEPS de combustibles se actualizarán conforme a la inflación, por lo que entre 2017 y 2018, dichas cuotas pasaron de 4.30 a 4.59 pesos por litros de Magna, de 3.64 a 3.88 pesos por litro de Premium; y de 4.73 a 5.04 pesos por litro de diesel.

- Paulo Cantillo