Boletín
FINANCIERO
Seguro de Crédito y Líneas Financieras

LOCKTON®

Septiembre 2017

Economía y seguro de credito

FUENTE: Aseguradora de Crédito, Solunion, Septiembre 2017

Las cifras apuntan a la mayor aceleración del crecimiento del PIB mundial en los últimos dos años, en el primer semestre de 2017. A pesar de ello, algunos de los motores económicos mundiales parecen no estar a punto.

El momento de crecimiento es bueno, en un contexto que incluye unos Estados Unidos decepcionantes, un pronóstico alentador para Europa y una estabilización de los países emergentes. El crecimiento del PIB mundial se calcula en un +2,9% para 2017 y 2018, el séptimo año consecutivo por debajo del 3%. Se han hecho revisiones al alza para la eurozona (+0,2pp, hasta el +1,9%), China (+0,4pp, hasta el +6,7%) y Japón (+0,1pp hasta el +1,3%). En contraposición, se han llevado a cabo revisiones a la baja para Estados Unidos (-0,1pp, hasta el +2,2%), Latinoamérica (-0,2pp, hasta +1,2%), Oriente Medio (-0,2pp hasta +2,1%) y Sudáfrica (-0,4pp, hasta +0,6%).

El crecimiento del PIB mundial se está acelerando a buen ritmo y ha alcanzado su máximo en dos años. Sin embargo, tras este contexto positivo se esconden marcadas divergencias económicas entre países. Mientras el crecimiento del PIB ha sido mediocre en Estados Unidos, en China ha sido más fuerte y también se ha mantenido firme en la eurozona, especialmente por el crecimiento de las exportaciones. La confianza empresarial también ha mejorado notablemente, una vez que las compañías están percibiendo el impulso de una mayor demanda y la mejora del poder adquisitivo, tras varios años de lento crecimiento. Esta fuerte confianza empresarial también anuncia un crecimiento continuo de la inversión y la mejora progresiva de los mercados laborales. La combinación debería estimular el gasto privado.

El análisis identifica cinco aceleradores del PIB mundial, así como cinco amenazas para el crecimiento de calidad.

Economía y seguro de credito

FUENTE: Aseguradora de Crédito, Solunion, Septiembre 2017

Cinco impulsores del crecimiento de la economía mundial

- **Inflación** – impulsar la confianza y la inversión. La inflación se ha recuperado parcialmente con el repunte de los precios en 2017, especialmente gracias a la subida de las materias primas. Se espera un ritmo moderado en la tendencia de reactivación.

- **Aumento del consumo y la inversión** – las ventas al por menor han crecido a nivel mundial, especialmente en Estados Unidos y China, además de registrar un buen ritmo de crecimiento en la eurozona donde los niveles de confianza no tienen precedentes. El ciclo de la inversión también se está recuperando.

- **Aceleración del comercio de exportación** – las exportaciones mundiales continuaron recuperándose en el primer semestre de 2017, tanto en términos de volumen como de valor, tras dos años de contracción en este último Las exportaciones de bienes a nivel mundial aumentaron un +2,3% interanual en abril de 2017.

- **Políticas de apoyo** – Como la liquidez mundial alcanzó niveles récord (por encima de los 19 trillones de dólares), se deberían mantener las numerosas políticas monetarias acomodaticias a pesar de los ajustes en los balances contables.

- **Riesgo político** – en general, la percepción de riesgo político se ha suavizado, salvo por los bandazos de Estados Unidos, cuya influencia en el impulso del crecimiento podría haberse subestimado.

Economía y seguro de credito

FUENTE: Aseguradora de Crédito, Solunion, Septiembre 2017

Cinco riesgos mundiales para la calidad del crecimiento

- **La reflación podría generar un efecto negativo** – mientras la reflación es actualmente positiva para la facturación de las empresas y el consumo de los hogares, hay riesgo de que los márgenes y el poder adquisitivo reaccionen de manera negativa.

- **El ciclo de la inversión está ampliamente financiado con deuda** – la vuelta a la normalidad de la actividad económica conlleva riesgos para alcanzar picos de crecimiento. En Estados Unidos, por ejemplo, una cifra récord de pedidos y empleos combinada con unos niveles mayores de deuda privada podrían resultar en una desaceleración para el final de 2017, sin un estímulo fiscal importante. También preocupan el aumento de los niveles de deuda en Europa (deuda pública) y en los principales mercados emergentes (deuda privada). El aumento de los tipos de interés podría comprometer el ciclo de la inversión, especialmente en los mercados en los que los niveles de deuda ya son elevados. Latinoamérica y los países asiáticos serían especialmente sensibles.

- **Proteccionismo** – el proteccionismo no está remitiendo, aunque el número de nuevas medidas proteccionistas se está estabilizando, incluyendo Argentina, India, Rusia y Estados Unidos.

- **Un pinchazo causado por una nueva crisis** – los gobiernos están centrados en los riesgos derivados de la falta de margen de maniobra suficiente para hacer frente a la próxima crisis. Además, el fracaso de las políticas podría generar un estrés financiero importante en Europa, especialmente en Italia, así como en Estados Unidos.

- **El riesgo político y los mercados podrían reconectar pronto** – tras el riesgo político récord alcanzado en Europa, Estados Unidos ha tomado ahora el protagonismo. En Europa no se esperan grandes crisis financieras o políticas, aunque la incertidumbre en el Reino Unido seguirá fomentando la volatilidad financiera mientras continúen las negociaciones del Brexit. Se espera que el crecimiento del PIB siga siendo suave (+1,4% en 2017; +1,0% en 2018), mientras aumenta la sensación del consumidor de pérdida de poder adquisitivo real.

Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

La impresora de la oficina: ¿un punto débil en su estrategia de seguridad?

"Primero me hice con el control de sus impresoras. Después, con el de su red. A continuación, con sus datos... Y no es lo único que he robado en esta empresa. Esta gente tiene todas las papeletas para pasarlo muy mal".

Esto es un extracto del cortometraje El lobo, producido por HP y protagonizado por Christian Slater. El lobo muestra cómo una inocente impresora de oficina, la primera "cosa" del Internet de las cosas (IoT, por sus siglas en inglés), puede llegar a ser una amenaza de seguridad por la que introducirse fácilmente.

❖ Abierto de par en par

Hoy en día, la mayoría de las impresoras están conectadas vía wifi. En muchas de ellas la conexión está abierta por defecto, lo que equivale a aparcar un Ferrari en un garaje y anunciar con un letrero luminoso que está ahí, que la puerta está abierta y que las llaves están en la guantera.

❖ ¿Le suena exagerado?

En 2009 se lanzó al mercado el programa Shodan, diseñado para detectar dispositivos conectados a Internet, en particular aquellos con fallos de seguridad. Shodan despertó mucho interés cuando se supo que era capaz de encontrar webcams vulnerables, lo que permitía a los hackers acceder a imágenes de vídeo sin que los dueños de los aparatos se den cuenta.

Recientemente unos investigadores han desarrollado en Singapur dos aplicaciones móviles basadas en Shodan que buscan dispositivos wifi abiertos. Las impresoras son el principal objetivo. La idea consiste en equipar un dron con un smartphone que tenga instalada una de estas aplicaciones y utilizarlo para buscar conexiones wifi abiertas en edificios de oficinas.

Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

Una de las versiones, llamada Cybersecurity Patrol, es benévola. Cuando la aplicación encuentra una impresora abierta, crea un punto de acceso falso y envía un mensaje de advertencia a la impresora para alertar a la empresa de su vulnerabilidad.

Con la versión malévola, el punto de acceso falso puede usarse para interceptar documentos dirigidos a la impresora. Dichos documentos, que pueden contener información confidencial o privada, pueden enviarse a la cuenta Dropbox del hacker gracias a la conexión 3G o 4G del teléfono. Una vez descargados, la aplicación puede reenviarlos a la impresora "real" para que nadie se percate de la intrusión.

Además de para la extracción directa de datos, los hackers pueden utilizar las impresoras y fotocopiadoras para acceder a todo el servidor de archivos de la empresa. Empleando el dispositivo comprometido como puente, los cibercriminales son capaces de instalar un malware en la red de la empresa y causar daños de todo tipo, filtrar datos o incluir la red en una botnet para perpetrar un ataque de denegación de servicio distribuido (DDoS).

❖ Tome medidas

Las redes wifi desprotegidas no son la única vía de acceso a los sistemas y datos de la empresa a través de las impresoras.

❖ Dé la voz de alarma

Aunque los métodos que utilizan los hackers para introducirse a través de las impresoras son de sobra conocidos, las amenazas de seguridad a menudo se pasan por alto.

Según un estudio del Instituto Ponemon publicado en 2015, el 56 % de las empresas no incluye a las impresoras de oficina en los análisis de seguridad. Resulta aún más llamativo que nada menos que un 60 % hayan sufrido una filtración de datos a través de la impresora y tardaron una media de 46 días en resolver el problema.

Es más, según un estudio de HP publicado en 2016, solo el 18 % de los encuestados mostraron preocupación por la seguridad de sus impresoras, mientras que el 91 % se mostró preocupado por la seguridad de sus ordenadores.

Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

❖ Reconocer la amenaza

Proteger una impresora de los hackers no cuesta demasiado trabajo y a menudo basta con tomar medidas básicas y de sentido común. Lo más difícil suele ser garantizar que las impresoras de red se incluyan en los programas de ciberseguridad.

Los expertos en seguridad recomiendan a las empresas que solo adquieran dispositivos con funciones de seguridad integradas, como software de detección. Cada vez son más los modelos de impresoras que incluyen potentes medidas de seguridad, pero sigue habiendo muchos que carecen de ellas.

Otra medida consiste en analizar qué dispositivos están conectados a su red. Con la ayuda de un inventario exhaustivo, los encargados de seguridad pueden desconectar los dispositivos que no requieren conexión a Internet y tomar las precauciones necesarias respecto a los que sí (por ejemplo, cambiar la conexión inalámbrica a una por cable siempre que sea posible).

Además, se deben cambiar siempre las contraseñas por defecto cuando se incorpore un nuevo dispositivo a la infraestructura de la empresa. Mientras que en los ordenadores es habitual hacerlo, los periféricos como las impresoras, los aparatos de aire acondicionado y las cámaras de circuito cerrado suelen funcionar con la contraseña de administrador proporcionada por el fabricante.

Por último, como ocurre con todos los ciberriesgos, es importante saber que la tecnología de seguridad tiene sus límites. Las empresas pueden aplicar los últimos sistemas y procedimientos de seguridad, pero la clave para reducir las amenazas siguen siendo los usuarios.

Riesgos Cibernéticos

FUENTE: William A. Boeck, SVP, Insurance & Claims Counsel, Lockton Financial Services, Cyber Technology Practice.

La vulneración de Datos de Equifax

Para estos momentos, todos los que están leyendo este blog son conscientes de la violación de datos sufrida por Equifax, Inc. "Catastrophic", "básicamente el Irma de las violaciones de datos", "la peor violación de datos jamás", los superlativos han llegado rápido y furioso en estos días,. No importa qué palabras usted prefiera, la brecha es un acontecimiento serio que exige la atención. Estoy reimprimiendo el texto de una alerta de Michael Born de la Práctica de Tecnología Cibernética de Lockton publicado hoy que revisa la violación y sus ramificaciones con el fin de ayudar a las empresas y los individuos con su respuesta.

¿Qué Sucedió?

El pasado 7 de septiembre de 2017, Equifax Inc. (NYSE: EFX) anunció un incidente de ciberseguridad que podría afectar a aproximadamente 143 millones de consumidores estadounidenses y un número no especificado de ciudadanos británicos y canadienses. Los delincuentes explotaron una vulnerabilidad de la aplicación del sitio web de los Estados Unidos para obtener acceso a ciertos archivos entre mediados de mayo y julio de 2017. La información a la que se accedió incluía algunos o todos los elementos siguientes:

- Nombres
- Números de Seguro Social
- Fechas de nacimiento, direcciones
- Números de licencia de conducir
- Información de tarjeta de crédito
- Documentos de disputa de crédito con información de identificación personal
- Equifax no ha encontrado evidencia de actividad no autorizada en las bases de datos de informes de crédito comerciales o de consumidores centrales de Equifax.

Información adicional del caso:

Equifax recomienda que los consumidores con preguntas adicionales visiten www.equifaxsecurity2017.com o comuníquese con un centro de llamadas dedicado al 866-447-7559, que la compañía estableció para ayudar a los consumidores. El centro de llamadas está abierto todos los días (incluidos los fines de semana) de 7:00 a.m.-1: 00 am hora del Este.

Riesgos Cibernéticos

FUENTE: William A. Boeck, SVP, Insurance & Claims Counsel, Lockton Financial Services, Cyber Technology Practice.

Próximos pasos a seguir

❖ Consumidores Individuales

Equifax alienta a los consumidores a revisar su sitio web especifico, www.equifaxsecurity2017.com, para determinar si su información ha sido potencialmente afectada. El sitio también ofrece a los consumidores de EE.UU. la oportunidad de inscribirse para el seguimiento de archivos de crédito y la protección contra el robo de identidad. La oferta, llamada TrustedID Premier, incluye tres monitoreo de crédito de la oficina de Equifax, Experian y TransUnion informes de crédito; copias de los informes de crédito de Equifax; la capacidad de bloquear y desbloquear los informes de crédito de Equifax; seguro de robo de identidad; y escaneo de Internet para los números de Seguro Social. El servicio TrustedID Premier se proporciona de forma gratuita durante un año a todos los consumidores de EE.UU., independientemente de si su información se vio comprometida en caso de incumplimiento. El sitio web también proporciona información adicional sobre las medidas que los consumidores pueden tomar para proteger su información personal.

Se ha informado de que los términos de uso de los servicios de monitoreo de crédito y protección contra robo de identidad ofrecidos por Equifax incluyen la liberación de los derechos de los individuos a participar en una demanda colectiva y les obliga a arbitrar cualquier disputa relacionada con la violación. Equifax ha aclarado desde entonces que la cláusula de arbitraje y la renuncia de acción colectiva en los términos de uso se aplican sólo a los servicios prestados y que no limitan los derechos que los consumidores pueden tener como resultado de la violación de datos.

Además de la página web, Equifax enviará avisos de correo directo a los consumidores cuyos números de tarjeta de crédito o documentos de disputas con información de identificación personal se vieron afectados.

❖ Empresas que utilizan los servicios de Equifax

Equifax ofrece muchos servicios a las empresas, incluyendo la gestión de la Ley del Cuidado de Salud a Bajo Precio, soluciones de pago sin papel y análisis de la cuenta del cliente. Si su empresa utiliza cualquier servicio de Equifax, puede haber proporcionado información confidencial y personal sobre empleados o clientes a Equifax y no está claro si esta información fue o no afectada por la vulneración

La estrategia para su respuesta, si la hay, debe ser coordinada entre sus recursos legales internos y externos.