Antonio Ramos, CISA, CISM, CRISC, CCSK, es el fundador de Leet Security, la primera agencia de calificación en la UE y Presidente del Capítulo de Madrid de ISACA. Con más de 14 años de experiencia, Antonio se ha especializado en el gobierno de la seguridad, planificación estratégica de protección de infraestructuras críticas, ciberseguridad y computación en la nube. Puede ser localizado en *antonio.ramos@leetsecurity.com.*

Etiquetado de seguridad de los servicios de TI utilizando una metodología de calificación

CONTEXTO

La subcontratación de ciertas funciones de TI ha sido común durante las últimas décadas (desarrollo, *housing, hosting y outsourcing*), pero la irrupción de la computación en la nube lo ha llevado a un nuevo nivel. Y, aunque algunos puedan pensar que la computación en la nube es solo una evolución del *outsourcing* es, de hecho, un nuevo paradigma que está cambiando la forma de acercarse a las TI. En lugar de algo que las organizaciones hacen por sí mismas, TI se está convirtiendo en un servicio que las organizaciones consumen (de forma similar a lo que ocurrió con el suministro energético en la revolución industrial).

Los profesionales de la seguridad han sido conscientes desde hace tiempo de que la subcontratación no elimina los riesgos de TI a los que la organización se enfrenta; de hecho, con la subcontratación, las organizaciones pierden el control sobre alguna de las medidas de seguridad implementadas por los proveedores de servicio. Por este motivo, para construir relaciones de confianza con dichos proveedores de servicio los profesionales de seguridad han aplicado una receta basada en auditorías y certificaciones.

Sin embargo, este enfoque debe cambiar para ajustarse al nuevo paradigma de la nube ya que, a pesar de las auditorías y las certificaciones, los usuarios continúan pensando que hace falta más transparencia:

> *"Entre los factores limitantes [de la computación en la nube], la seguridad y la propiedad de los datos (ambos relacionados con la capacidad de proteger los activos de información) y los factores relacionados con aspectos legales, contratos y cumplimiento regulatorio encabezaban la lista. El quinto factor, la garantía de la información, es significativo porque está relacionado con la transparencia de la oferta de servicios en la nube y la capacidad de la dirección para obtener el consuelo de que su información está protegida hasta el punto necesario"*[1]

Es decir, aunque los profesionales de la seguridad han estado aplicando mejores prácticas y pidiendo auditorías y certificaciones de seguridad, estos mecanismos no han sido capaces de transmitir el nivel de confianza necesario exigido por los clientes de servicios de computación en la nube.

¿FALLAN REALMENTE LAS AUDITORÍAS Y LAS CERTIFICACIONES EN PROPORCIONAR TRANSPARENCIA?

Las auditorías y certificaciones de seguridad son las bases de la creación de confianza entre clientes y proveedores, pero tienen algunas características que obligan al desarrollo de mecanismos adicionales:

- Los informes de auditoría típicos no pueden ser distribuidos libremente; solo son para las partes implicadas (normalmente, el cliente y el proveedor), lo que obliga al proveedor a ser auditado por cada (potencial) cliente.
- Los informes SOC (*Service Organization Control*) pueden ser publicados, pero aparecen otros inconvenientes: Los criterios utilizados por el auditor pueden ser o no relevantes para los clientes, puesto que han sido fijados por una tercera parte. Si los criterios no son relevantes para los clientes, el punto anterior vuelve a ser de aplicación.
- Finalmente, en relación con las certificaciones, no existe certificación para la seguridad de los servicios. Lo que los proveedores están certificando es su *Sistema de Gestión de la Seguridad de la Información* respecto al estándar ISO/IEC 27001. Estas certificaciones tienen dos inconvenientes:
  1. No dicen nada sobre las medidas de seguridad implementadas por el proveedor; indica solamente si el proveedor tiene un sistema de gestión de seguridad de la información.

2. Obliga al cliente a comprender el alcance de la certificación porque podría no ser relevante para el servicio que quiere suscribir.

Por supuesto, un proveedor que implementa un sistema de gestión de seguridad de la información (SGSI) certificado sigue unas mejores prácticas y adopta medidas de seguridad siguiendo un proceso de gestión de riesgos, pero el cliente no puede derivar la robustez de las medidas de seguridad que el proveedor implementa a partir de la certificación exclusivamente. La certificación solo da una información muy sencilla: que el proveedor implementa un SGSI siguiendo la ISO/IEC 27001.

Por el momento, las herramientas que tienen los profesionales de seguridad, obligan a los clientes a ser especialistas de seguridad para comprender sus resultados y no proporcionan resultados comparables.

Catherine Aston, Alto Representante de la Unión Europea para Asuntos Externos, ha resaltado este mismo aspecto e invita a la industria a "desarrollar estándares liderados por la industria sobre el rendimiento de la ciberseguridad y mejorar la información disponible al público mediante el desarrollo de etiquetas de seguridad o marcas que ayuden al consumidor a navegar el mercado"[2].

UNA NUEVA HERRAMIENTA: LA CALIFICACIÓN

Explorar la teoría económica que explica las relaciones entre clientes y proveedores puede ser útil para identificar nuevas vías de construir confianza en el mercado de servicios en la nube. De hecho, la seguridad de los servicios en la nube (o si se prefiere, la ciberseguridad) se enfrentan a un problema bien conocido: la asimetría de la información.

Este concepto fue explicado por George Akerlof en 1970[3] y hace referencia a las "decisiones en transacciones en las que una parte tiene más o mejor información que la otra", que es exactamente lo que ocurre en el mercado de servicios de nube en relación con la seguridad: El proveedor tiene mejor información sobre las medidas de seguridad implementadas que el cliente.

La asimetría de la información crea un desequilibrio de poder que puede ocasionar que en algunas ocasiones la transacción salga mal. Los problemas más comunes que surgen son la selección adversa[4] y el riesgo moral.[5] No obstante, la peor consecuencia que la asimetría de la información podría tener sería la desaparición del mercado.

Los economistas Michael Spence y Joseph E. Stiglitz han analizado las dos principales soluciones a este problema:

- **Señalamiento (o signaling[6])**—El señalamiento significa que una parte (en este caso, el proveedor de servicios en la nube) transmite credibilidad sobre sí misma a la otra parte (el consumidor). Esto podría sonar un poco extraño, pero los profesionales de seguridad están muy familiarizados con este tipo de mecanismos, al que llamamos certificación de seguridad, y que proporciona un sello que las organizaciones pueden usar para señalar que cumplen con un conjunto de requerimientos.
- **Escaneado (o screening[7])**—El escaneador (aquel con menos información; en este caso, el cliente) intenta corregir la asimetría aprendiendo todo lo que puede sobre el proveedor. De nuevo, puede sonar extraño, pero los profesionales de la seguridad lo usan continuamente; lo denominamos auditoría.

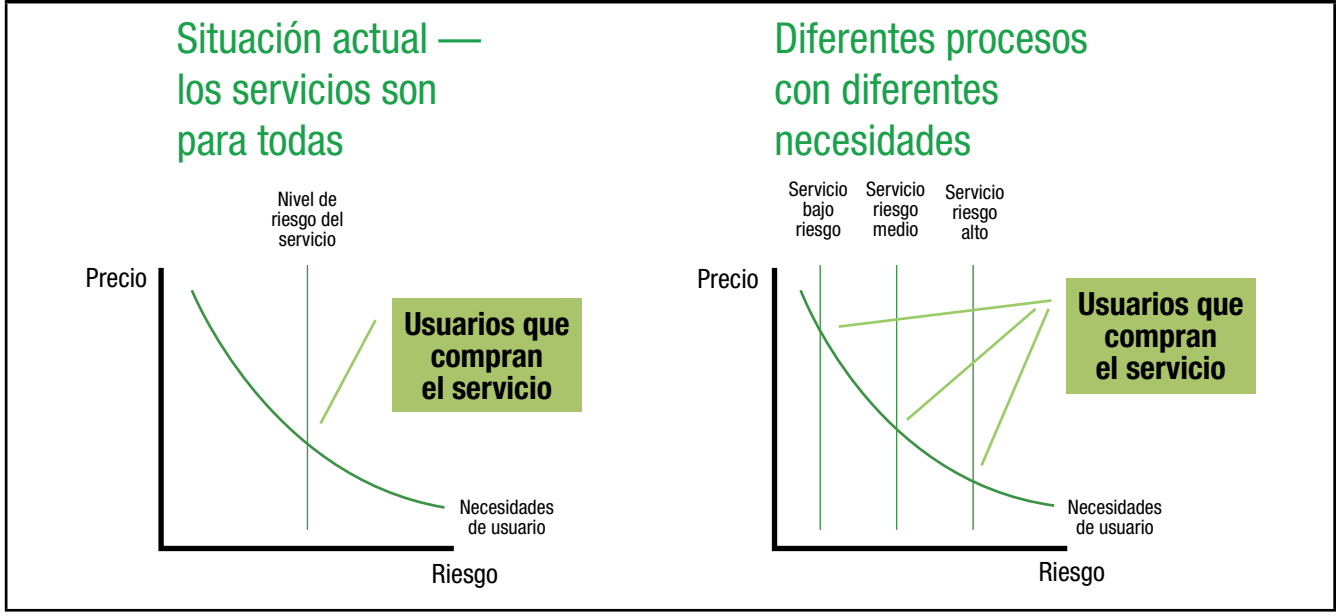
Una vez que se ha comprendido la teoría económica subyacente,[8] ¿existe otra opción para construir relaciones de confianza?

Efectivamente, existen alternativas en el mundo de la economía. El mismo problema sobre asimetría de la información que el mercado de servicios en la nube afronta actualmente ocurrió, por ejemplo, en el comienzo de los mercados de deuda. En aquellos días, los inversores estaban en una posición débil en relación a las compañías que solicitaban financiación: No conocían con qué probabilidad los deudores iban a devolver el crédito. Entonces, las agencias de calificación de deuda comenzaron a calificar a los deudores como un mecanismo de señalamiento.

ETIQUETAS DE SEGURIDAD UTILIZANDO UNA METODOLOGÍA DE CALIFICACIÓN

Utilizando estos conceptos del mundo de la economía en el campo de la seguridad, se puede implementar un sistema de etiquetado de la seguridad de los servicios de TI. Este sistema ayudaría a los (potenciales) clientes a entender fácilmente las características de seguridad de los servicios en el mercado y analizar si se ajustan a sus necesidades conforme a su perfil de riesgo (ver **figura 1**)—de la misma forma que los electrodomésticos son calificados de acuerdo a su consumo de energía o los vehículos son calificados según su seguridad. El sistema de etiquetado es también más eficiente, porque todos los clientes que quieran suscribir un servicio no necesitan auditar los controles de seguridad debido al enfoque "auditar una vez, usar muchas veces" (al estilo de lo que hace FedRamp[9]).

Figura 1—El Etiquetado Permite Ajustarse a Diferentes Necesidades de Usuario



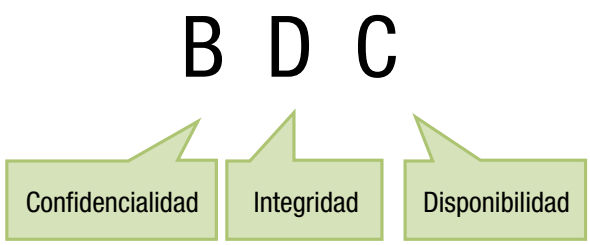
Calificar las medidas de seguridad en, por ejemplo, cinco niveles (de la A a la E, siendo A lo mejor) en las diferentes dimensiones de la ciberseguridad (confidencialidad, integridad y disponibilidad [CIA]) nos proporcionaría 125 posibles calificaciones diferentes (cinco niveles, tres dimensiones) que ayudaría a los clientes a elegir aquellos servicios que mejor se ajusten a sus necesidades. A diferencia de la certificación, que divide a todos los proveedores en dos grupos: aquellos que están certificados y los que no.

El resultado de la metodología de calificación sería un conjunto de tres letras indicando la robustez de las medidas de seguridad implementadas por el proveedor en cada servicio concreto en las mencionadas dimensiones de seguridad. Por ejemplo, una calificación BDC significa (**figura 2**):

- Una calificación B en la dimensión de confidencialidad
- Una calificación D en la dimensión de integridad
- Una calificación C en la dimensión de disponibilidad

En este ejemplo, el servicio presta una mayor atención a los aspectos de confidencialidad, pero no es adecuado para aquellos con unos requisitos de disponibilidad elevados (que deberían buscar una calificación de B o A en la tercera dimensión).

Figura 2—Calificación en Tres Dimensiones de Seguridad



La calificación (de servicios, no de proveedores) proporciona un valor relativo que puede ser entendido como una previsión de la solvencia técnica del vendedor en relación a su seguridad y resiliencia. De esta manera, los servicios con una mejor calificación tendrían una menor probabilidad de sufrir un incidente que afecte de manera significativa a los acuerdos de nivel de servicio.

CONSTRUYENDO EL SISTEMA DE CALIFICACIÓN

El primer paso para construir un sistema de calificación es crear un sistema para asignar un nivel (de la A a la E) a las medidas de seguridad implementadas por el proveedor. Para hacer esto, se deben realizar dos tareas:

1. **Elaborar un inventario de las medidas de seguridad a ser evaluadas.** Esta tarea debe realizarse partiendo de estándares, controles y marcos generalmente aceptados (p.ej., estándares del National Institute of Standards and Technology [NIST], ISO 27002, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago [Payment Card Industry Data Security Standard, PCI DSS], ITIL, la Directiva de Privacidad de la Unión Europea.)
2. **Definir los cinco niveles para cada medida de seguridad.** Esta definición tiene dos componentes: (i) Las medidas de seguridad que son procesos son calificados de acuerdo a su nivel de madurez (de manera similar a COBIT® 5 Process Assessment Model); y (ii) Las medidas de seguridad que dependen de la tecnología (p.ej., configuraciones de seguridad, herramientas) son calificadas de acuerdo a su robustez (p.ej., una contraseña de 12 caracteres es más robusta que otra de seis caracteres, y una contraseña de 12 caracteres es más robusta si requiere una combinación de letras, números y caracteres especiales).

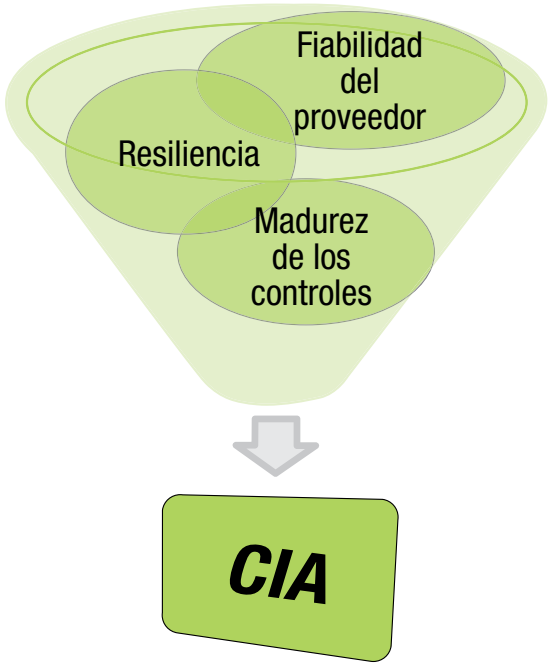
Además de la madurez de los controles de seguridad (analizado previamente), hay otros elementos que deberían ser considerados en la metodología para construir el sistema de etiquetado de la seguridad porque contribuyen a crear relaciones de confianza (**figura 3**):

- **Fiabilidad del proveedor**—Información relacionada con la estrategia del proveedor del servicio incluyendo planes de negocio, estabilidad financiera, órganos de gestión, hoja de ruta del servicio y cualificación de los empleados.
- **Resiliencia**—La capacidad del proveedor de recuperarse en caso de incidentes.

CONCLUSIONES

Las auditorías y calificaciones de seguridad son condiciones necesarias, pero no suficientes, para construir relaciones de confianza en el ciberespacio. Los profesionales de seguridad deben dar un paso adelante y proponer nuevas vías para evaluar la seguridad y resiliencia de los servicios de TI y estar preparados para nuevos escenarios tales como los originados por la computación en la nube y la ciberseguridad. En esta situación, el etiquetado de la seguridad basado en una metodología de calificación podría, por ejemplo, ayudar a los usuarios a entender el riesgo al que se enfrentan cuando usan diferentes servicios de TI, a comparar diferentes opciones y a ser más eficientes en los procesos de adquisición.

Figura 3—Elementos a Considerar en la Metodología de Calificación



NOTAS AL PIE

[1] "2012 Cloud Computing Market Maturity. Study Results", ISACA y Cloud Security Alliance, USA, 2012

[2] Alto Representante de la Unión Europea para Asuntos Externos y Política de Seguridad, *"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberespace"*, JOIN (2013) 1 final, Bélgica, 7 de febrero de 2013

[3] Akerlof, George; *The Market for Lemons: Quality Uncertainty and the Market Mechanism*, 1970

[4] La selección adversa "hace referencia al proceso de mercado en el que ocurren resultados no deseados cuando compradores y vendedores tienen información asimétrica (acceso a información diferente); es más probable que los productos o servicios 'malos' sean elegidos." Chandler, Seth J.: "Adverse Selection", The Wolfram Demonstrations Project

[5] Un riesgo moral es una "situación en la que una parte tendrá tendencia a asumir riesgos porque el coste en el que podría incurrir no lo notaría la parte que asume el riesgo. En otras palabras, es una tendencia a estar más dispuesto a asumir un riesgo sabiendo que el coste potencial de sufrir o asumir dicho riesgo serán asumidos, en su totalidad o en parte, por otros." Dembe, Allard E.; Leslie, I. Boden; "Moral Hazard: A Question of Morality?", *New Solutions*, 10(3), 2000, p. 257-279

[6] Spence, Michael; "Job Market Signaling", *The Quarterly Journal of Economics*, vol. 87, no. 3, 1973

[7] En el escaneado, "la parte menos informada puede inducir a la otra parte a revelar su información. Pueden proporcionar un menú de opciones de forma que la elección dependa de la información privada de la otra parte." Stiglitz, Joseph E.; "There Is No Invisible Hand," The Guardian Comment, UK, 20 de diciembre de 2002

[8] En 2001, el Premio Nobel en Economía fue para George Akerlof, Michael Spence y Joseph E. Stiglitz por su "análisis de los mercados con información asimétrica".

[9] Federal Risk and Authorization Management Program, *www.fedramp.gov*

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.