



¿QUÉ  
PREOCUPA?

## EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN A PROVEEDORES

Muchas compañías están preocupadas por la Seguridad de la Información y, por ello, han implementado estándares, políticas y procedimientos específicos. Todo esto suele ir acompañado de controles, auto-evaluaciones, auditorías, etc. Por otro lado, cada vez es más común que las empresas contraten ciertos servicios con proveedores externos. Algunos de estos servicios requieren que el proveedor acceda a información clasificada como confidencial e, incluso, es posible que tenga que almacenarla y/o procesarla; pero, ¿qué ocurre con la Seguridad de la Información en este caso? ¿Qué se debe hacer?

### Razones para trabajar con proveedores

Es un hecho que cada vez se contratan más servicios sensibles con terceros. Hay diversas razones para ello, y cada compañía tiene las suyas. A continuación se muestran algunos ejemplos que pueden motivarlo:

- **Proveedores especializados en una determinada funcionalidad:** Podemos pensar, por ejemplo, en un *Call Center* para realizar campañas de marketing a clientes, en un

fidencialidad, integridad y disponibilidad de los datos, en correspondencia con el servicio y el tipo de información manejada.

Otra razón no menos importante son los requerimientos legales. Cada vez hay más leyes que enfatizan la importancia de que debemos proteger la información de nuestros clientes. Concretamente, las empresas financieras norteamericanas están sujetas a leyes como:

- 1999 Gramm-Leach-Bliley Act (GLBA).
- 2003 Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbooks.

### Razones para crear un Proceso de Evaluación de la S.I. a proveedores

- Asegurar de manera razonable que se aplicarán medidas adecuadas para proteger la información
- Cumplir con requerimientos legales:
  - 1999 Gramm-Leach-Bliley Act (GLBA) en USA
  - 2003 Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbooks (USA)
  - RD 1720/2007 Reglamento de desarrollo de la LOPD (España)
- Políticas y Procedimientos de la Corporación
- Centrarnos en las áreas de negocio de alto riesgo
- Mitigar los riesgos del negocio
- Asegurar la consistencia de las evaluaciones (actuar con el mismo criterio en toda la Corporación)
- Tener un modelo global
- Tener un proceso centralizado: Base de Datos global
- Ahorrar tiempo y dinero al eliminar evaluaciones duplicadas

puso en marcha en 2005 y tiene los siguientes beneficios:

- Hacer una evaluación de cómo el proveedor va a manejar nuestros datos para poder asegurar de una manera razonable que la información se va a proteger de forma adecuada de acuerdo con el servicio y tipo de información.
- Poner la atención en las áreas de negocio de alto riesgo.
- Mitigar los riesgos del negocio identificados en este proceso.
- Asegurar la consistencia de las evaluaciones.
- Contar con un modelo global que permita a la casa matriz tener el control de la evaluación realizada a cualquier proveedor.
- Ahorrar tiempo y dinero al eliminar evaluaciones duplicadas: si un proveedor da servicio a diferentes negocios de la corporación, será suficiente con una evaluación que cubra todos los servicios; y no será necesario que cada negocio haga la suya. Esto hace que el proceso sea más eficaz y eficiente.
- Cumplir con los requerimientos legales.

### Proceso de Evaluación de Seguridad de la Información a Proveedores

A continuación se muestran una serie de indicaciones sobre este posible proceso basado en la experiencia de Citi.

Para controlar que todos los proveedores "afectados" pasan por este proceso, se dispone de una base de datos corporativa y centralizada. Cuando cualquier empresa del grupo contrata un nuevo proveedor, en cualquier parte del mundo, debe declararlo en esta base de datos y determinar si hay que realizar esta evaluación.

En Citi este proceso se aplica a todos los proveedores que manejan información confidencial. Hay algunas excepciones, como abogados o instituciones financieras reguladas, donde se considera que, bien por su código ético y/o controles, gestionan correctamente la información y no es necesario realizar la evaluación. En cualquier caso, se deben documentar y formalizar todas las excepciones.

También se debe contemplar que pueden darse circunstancias que hagan dudar de la validez de una evaluación realizada, y se recomienda hacer una extraordinaria. Algunas de estas circunstancias podrían ser:

- *Ha habido un incidente de seguridad.*
- *Hay un cambio de propietario del proveedor que pudiera ocasionar un cambio en*

No tiene sentido que en nuestra empresa pongamos tantas medidas de seguridad y controles para asegurarnos de que los datos sensibles se manejan adecuadamente, y no sepamos qué es lo que ocurre cuando el servicio se realiza fuera de la casa.

servicio de almacenamiento de información confidencial (documentos que tienen que guardarse por requerimiento legal durante bastantes años, como pueden ser contratos físicos con clientes, etc.), servicio de destrucción de información confidencial, etc.

- **Proveedores que proporcionan un servicio a bajo coste:** Como ejemplo podemos pensar en compañías de software en otros países como India o Singapur, y en servicios proporcionados desde Latinoamérica.

### Razones para crear un proceso de evaluación de Seguridad de la Información a proveedores

No tiene sentido que en nuestra empresa pongamos tantas medidas de seguridad y controles para asegurarnos de que los datos sensibles se manejan adecuadamente, y no sepamos qué es lo que ocurre cuando el servicio se realiza fuera de la casa.

Debemos asegurarnos de que estos proveedores van a aplicar unas medidas de seguridad apropiadas para proteger la con-

En el caso de España, el Real Decreto 1720/2007 aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal, que en el Capítulo III (Encargado del Tratamiento), artículo 20 (Relaciones entre el responsable y el encargado del tratamiento) dice en el punto 2: "*Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar porque el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este reglamento*".

Una vez visto que se están externalizando servicios donde se maneja información confidencial, que es conveniente realizar una evaluación de Seguridad de la Información a dichos servicios, y que las políticas de S.I. son las mismas en todas las empresas del grupo independientemente de su localización, Citi ha decidido implementar un proceso formal común en toda la corporación.

Este proceso denominado TPISA (Third Party Information Security Assessment) se

las políticas de seguridad.

• El proveedor utiliza para el servicio a cuartas partes (no identificadas previamente) que manejan información confidencial de nuestra compañía.

### Equipo de la Evaluación de Seguridad de la Información

El equipo estará formado por los siguientes miembros:

• **Asesor Líder de Seguridad de la Información Certificado.** Será el encargado de liderar la evaluación. Debe ser una persona competente preparada especialmente para ello. En el caso de Citi, existe una certificación interna que permite realizar este trabajo. El objetivo es asegurar consistencia en las evaluaciones, y de esta manera, permitir que una evaluación realizada por un negocio sea válida para otro.

• **Responsable de la relación con el proveedor.** Es la persona de negocio que lleva la relación, y toma un rol muy activo en estas evaluaciones.

• **Responsable de Seguridad de la Información de Negocio.** Se encargará de formalizar los riesgos que se descubran en la evaluación, así como de hacer un seguimiento de sus planes de acción.

• **Expertos:** dependiendo del servicio proporcionado por el proveedor, así como de los conocimientos del Asesor Líder, se puede requerir que se incorporen al equipo expertos en diferentes materias: en seguridad física, en redes, etc.

Para conseguir realizar una buena evaluación, es necesaria la cooperación de todos los miembros del equipo y, en especial del responsable de la relación con el proveedor.

### Fases de una Evaluación de Seguridad de la Información a Proveedores

1.- **Toma de decisión sobre el tipo de evaluación.**

En el momento de la contratación, y dependiendo del proveedor, el servicio prestado y la criticidad, hay que determinar si es necesario o no realizar esta evaluación, y si ésta se debe acompañar de una visita a las instalaciones o si se puede hacer de forma remota.

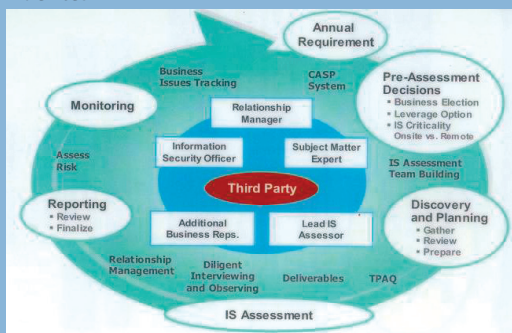
2.- **Descubriendo y Planeando.**

En esta fase, el Asesor Líder de Seguridad de la Información se reunirá con el responsable interno de la relación con el proveedor para recopilar toda la información que pueda resultar útil: datos sobre el servicio proporcionado, si hay otras unidades de negocio involucradas, si el proveedor subcontrata a cuartas partes para proporcionar el servicio, el contrato firmado, controles

que el negocio realiza sobre el proveedor (tanto si son para medir el nivel de servicio o por cualquier otra razón), etc.

A continuación se muestran una serie de temas que se pueden contemplar en un TPISA:

- Políticas y estándares.
- Identificación y autenticación.
- Autorización y controles de acceso.
- Confidencialidad e integridad.
- Detección y respuesta ante incidentes.



puntos de mayor riesgo para aclarar las posibles dudas que hayan surgido al revisar la documentación aportada. Se podrán ver las instalaciones del proveedor, y revisar *in situ* documentos, controles y actividades del día a día del proveedor que nos ayude al propósito de la evaluación.

Ante un no cumplimiento con la política de seguridad de nuestra compañía, se hará un análisis junto con el proveedor para determinar si hay algún tipo de riesgo.

Nunca hay que olvidar que nuestro objetivo no es que el proveedor cumpla con todas nuestras políticas, sino que nuestra información se gestione de una forma adecuada. Es perfectamente posible que el proveedor no cumpla con algunos puntos de la política y que esto no suponga un riesgo para nuestro servicio; bien por el tipo de servicio proporcionado, bien porque tenga otros controles diferentes.

De esta forma, si finalmente se

Ante un no cumplimiento con la política de Seguridad de la compañía, se hará un análisis junto con el proveedor para determinar si hay algún tipo de riesgo o no. Nunca hay que olvidar que nuestro objetivo no es que el proveedor cumpla con todas nuestras políticas, sino que nuestra información se gestione de una forma adecuada.

- Administración.
- Formación y concienciación.
- Cortafuegos y sistemas de detección de intrusos.
- Mantenimiento y desarrollo de aplicaciones.
- Seguridad física.
- Continuidad de negocio.
- Sub-contratistas.
- Cumplimiento con las leyes.
- Relación con el proveedor.
- Transporte de medios electrónicos.
- Mensajería segura.
- Información confidencial accesible desde Internet.

Una vez analizada toda la información, se determinarán las preguntas a realizar al proveedor, así como la documentación a solicitar. Esto será enviado al proveedor para que sus respuestas puedan ser analizadas antes de la visita.

En base al servicio proporcionado y a la revisión de las respuestas se determinará si se necesita algún experto en alguna materia para la siguiente fase.

3.- **Evaluación de Seguridad de la Información.**

Durante esta fase se tendrá una entrevista con el proveedor centrada en los

descubre algún tipo de riesgo, se solicitará al proveedor que prepare un plan de acción para mitigarlo o resolverlo.

4.- **Informe Final.**

Se preparará un informe final con las recomendaciones para resolver los riesgos que se hayan detectado en el servicio, y se solicitará una respuesta indicando el plan de acción y una fecha objetivo.

5.- **Monitorización: seguimiento de los problemas detectados.**

De la misma manera que haríamos con un riesgo de Seguridad de la Información en un proceso interno, se formalizarán los riesgos detectados en el proveedor y se hará un seguimiento de su estado hasta su resolución.

Por último, conviene indicar que este proceso de evaluación se debe repetir periódicamente y estar en continua mejora. ■



Luis Ballesteros Martín  
Director del Departamento de Seguridad de la Información y Continuidad de Negocio  
CITIBANK ESPAÑA  
luis.ballesteros@citi.com