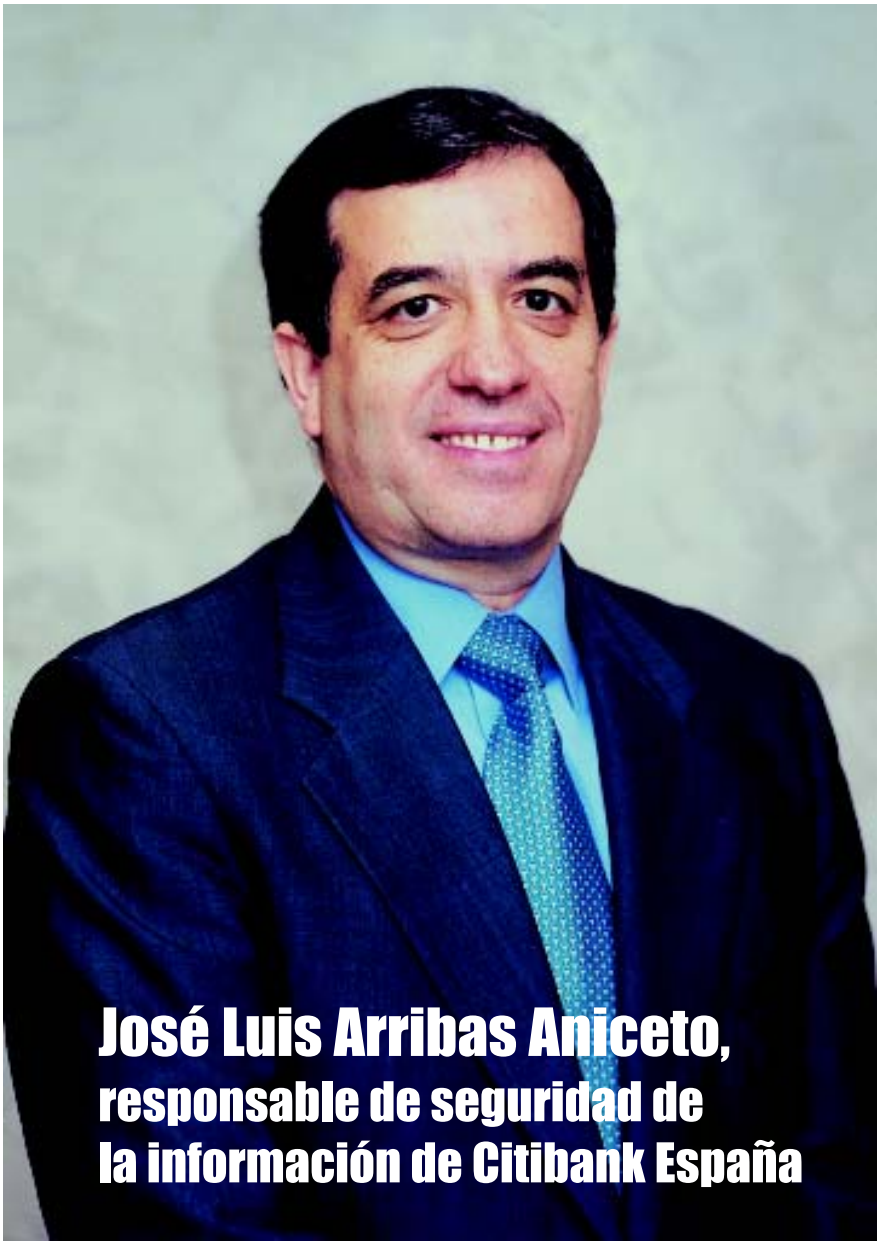
«Es necesario disponer de copias de seguridad de los datos fuera de los habituales centros de proceso o tratamiento»



José Luis Arribas Aniceto, responsable de seguridad de la información de Citibank España

La sabiduría en una disciplina, seguridad de la información incluida, suele ser producto de su estudio, de los años de práctica y de la experiencia de haber vivido situaciones difíciles. Estas tres condiciones concurren en José Luis Arribas Aniceto, responsable de seguridad de la información –*Business Information Security Office* (BISO)– de Citibank España, quien en esta entrevista realiza interesantes declaraciones sobre la organización de la seguridad de la información en su entidad y manifiesta algunas enseñanzas aprendidas tras los desgraciados acontecimientos del 11-S.

– ¿Qué se entiende en Citibank por seguridad de la información?

– En el ámbito teórico podríamos decir que es el conjunto de prácticas y procedimientos dirigidos a salvaguardar la información de nuestros clientes, empleados, proveedores, accionistas, etc., de cualquier tipo de amenaza, y que asegure el cumplimiento de las políticas de Citigroup y leyes o reglamentos aplicables (locales o comunitarios). Aquí incluyo lo relacionado con la protección, la privacidad de los datos y la continuidad, visto siempre desde la perspectiva de negocio y no únicamente desde la de la seguridad informática o de los sistemas de información tecnológicos.

A efectos prácticos podríamos decir que se concreta en el conjunto de medidas que aseguran en el día a día lo que indican los procedimientos, reglamentos y leyes. Aplicamos tales medidas a la información esté donde esté: sistemas informáticos, papel, en terceros, de tal suerte que siempre podamos conocer y/o asegurar quién usa nuestros servicios, la confidencialidad e integridad de la información, que estamos en disposición de prevenir los cambios no autorizados o el repudio de las transacciones, y si tenemos un problema, poder tomar la acción apropiada, minimizarlo y asegurar la disponibilidad de la información.

El cambio continuo de la tecnología, las amenazas y últimamente también de las leyes nos obliga a revisar de forma continua nuestra política de seguridad de la información, y también provoca que debamos hacer especial énfasis en la concienciación y formación de todos los participantes, sean técnicos, usuarios finales, clientes... No hay otro camino para conseguir que las buenas prácticas de seguridad de la información formen parte del día a día.

– ¿Cómo se estructura la organización de la seguridad de la información en Citibank a escala multinacional y a efectos domésticos en los distintos países en los que existe implantación, España por ejemplo?

– En 1995 se creó la Oficina Corporativa de Seguridad de la Información, CISO (*Corporate Information Security Office*), que es el centro de la organización de Citigroup en materia de seguridad. Está relacionado con las estructuras similares en materia de privacidad y de continuidad de negocio.

De CISO dependen unos treinta grupos regionales. En el correspondiente a Europa del Oeste cada país tiene un representante de dicha oficina, que es el denominado *Business Information Security Office* –BISO –, función que yo realizo para España y Portugal. Existen actualmente cerca de cuatrocientos BISO's en todo Citigroup.

El grupo regional en el ámbito de banca de consumo está formado por los BISO's de los diferentes países de Europa del Oeste, que mantienen reuniones periódicas para coordinar la política regional con soluciones comunes, dado que se utilizan arquitecturas similares, un mismo *Data Center*, así como las mis-

mas aplicaciones a nivel regional en la banca por Internet o el sistema de tarjetas de crédito.
Mientras que la oficina CISO se encuadra actualmente en el área tecnológica, en España BISO se integra en el grupo de Control y Auditoría Interna, reportando a la Dirección Financiera. Aquí somos independientes del grupo de Operaciones y Tecnología, aunque mantenemos una fuerte relación con él.
En realidad, la función del BISO no se centra exclusivamente en la seguridad informática, sino más ampliamente en asegurar la implantación de la seguridad de la información en el negocio. Nuestra responsabilidad es asegurarnos que la seguridad está imbuida en cada acción de negocio, asegurar a la organización de Citigroup que todas las iniciativas locales (proyectos, productos o servicios) son acordes con la política de seguridad corporativa, así como en las soluciones regionales en sus interfases con las locales.
Hay otro aspecto esencial relacionado con la concienciación. En nuestra organización, todos los empleados deben recibir información actualizada sobre seguridad de la información al menos con una periodicidad anual; concienciación e información que igualmente recibe cada nuevo empleado en la jornada de bienvenida junto a la relativa a la corporación y a sus estrategias del negocio.
El BISO tiene la responsabilidad sobre el seguimiento, información (al negocio y a la organización del CISO) y solución de cualquier tipo de amenazas o vulnerabilidades conocidas o detectadas, así como de todos los incumplimientos de las políticas, leyes o reglamentos y defectos o comentarios detectados en materia de seguridad de la información en cualquier tipo de auditoría o control.

– ¿Qué efectos ha tenido y está teniendo la desgraciada contingencia del 11-S en la concepción y el enfoque actuales de la seguridad de la información en Citibank?

– Nueva York es la ciudad origen de Citibank, y allí Citigroup tiene una importante presencia. Como es sabido, el WC7 era un edificio operativo de la corporación y su destrucción fue total como consecuencia del incendio y posterior derrumbe de las Torres Gemelas. El desastre afectó a más de 2.500 personas, que perdieron sus oficinas de trabajo, y hasta 16.000 se vieron desplazadas de sus centros en el bajo Manhattan. Hubo igualmente que lamentar la desaparición o pérdida de 6 vidas humanas por encontrarse en esos momentos de visita en las Torres o colaborando en las ayudas.
Unas 700 personas fueron reubicadas en oficinas de emergencia en el área de Nueva Yersey y las pérdidas estimadas por la corporación fueron de 700 millones de dólares. Citigroup, dentro de su plan de ayudas, ha creado diferentes fondos para colaborar y/o dirigir las ayudas a las familias de los afectados
En lo referente a la seguridad y continuidad de negocio, Citibank tenía en vigor las diferentes medidas de prevención y evacuación tal como se demostró, por lo que se pudieron seguir realizando las operaciones correspondientes a los edificios afectados desde los centros alternativos en unos plazos que variaron desde unas horas hasta los 3 días.

"Estamos afrontando la creación de una red de expertos técnicos en seguridad, los denominados TISO's –Technology Information Security Officers–, que nos permita una rápida respuesta ante incidentes y vulnerabilidades"

No obstante el 11-S ha servido para estudiar los planes en vigor, tomando consideraciones antes no apreciadas, como la alusiva a la concentración geográfica en una misma zona, y dando soluciones más regionales o globales que las dirigidas únicamente a las de un determinado local o edificio.
Con este fin, y de igual forma que en materia de seguridad de la información existe la organización CISO, se ha revisado a nivel local, regional y global la estructura de Continuidad de Negocio, mejorando la política y procedimientos en vigor y adaptándola a la necesidad de atender a este tipo de grandes desastres.
En España el presupuesto ya estaba adecuadamente contemplado y únicamente estamos revisando con más detalle su actividad. Hay que tener en cuenta que aquí, desde al menos el año 1988 en que se iniciaron las actividades relacionadas con la seguridad y continuidad, hemos tenido planes de contingencia en diferentes edificios, y disponemos desde entonces de locales alternativos, no sólo para la continuidad de las instalaciones informáticas, sino también espacio y equipos para el personal de Operaciones y de Negocio (marketing, finanzas, RRHH...) con más de 700 puestos de trabajo en edificios alternativos en Madrid y Barcelona, disponibles para su uso en caso de necesitarse.
Tal circunstancia en el ámbito local se dio en el 11-S, pues la dirección de la entidad en España, siguiendo las directrices de prevención que se marcaron para los intereses norteamericanos en dicha fecha, activó el Plan de Continuidad de Negocio en las instalaciones alternativas en Madrid. Durante cuatro días, este ejercicio 'real' nos sirvió para detectar unos cuantos defectos y, claro está, subsanarlos, lo que también ha sucedido en el contexto corporativo.

– ¿Cuál ha sido la enseñanza más importante que han sacado del 11-S?

– Que los datos hay que tenerlos. Los equipos destruidos fueron remplazados con la colaboración de los fabricantes y distribuidores, pero sin la existencia de copias de seguridad de datos no habría existido continuidad de negocio. Es necesario disponer de copias de los datos fuera de los habituales centros de proceso o tratamiento.

– ¿Utilizan internamente el mecanismo de firma electrónica?

– En Citigroup ya hemos establecido y tenemos en uso a nivel interno las herramientas o productos para firma electrónica, utilizándose inicialmente por los grupos ejecutivos o de dirección de negocio, y por profesionales de otras áreas que por su función necesitan disponer de este mecanismo: legal, cumplimiento, auditoría. También utilizamos firma electrónica en el intercambio de determinada información entre grupos de la corporación.

– ¿Podría comentar los proyectos de seguridad TIC más relevantes que se estén llevando a cabo o se tenga previsto realizar en Citibank?

– A nivel local estamos enfocados en la utilización de las tecnologías apropiadas para la gestión de los certificados digitales y correo seguro con los diferentes entes con los que nos relacionamos: clientes, proveedores, consultores, suministradores, etc.), mediante herramientas tecnológicas de Entrust y VeriSign. La intención es mantener la seguridad de nuestra red en los puntos débiles, es decir, en las conexiones

externas creadas a partir de la necesidad de que nuestros ejecutivos y empleados se conecten desde fuera de la red en sus viajes, o por necesidades de monitorización externa, resolución de incidentes, etc., así como nuestros colaboradores, consultores o proveedores, con especial énfasis en los procesos de externalización.

Otro proyecto en curso consiste en la implementación de cifrado Triple-DES en todos los elementos o procesos donde actualmente se mantiene el DES.

A nivel regional puedo mencionar el proyecto *Standard Operational Environment* (SOE) con el que se obtendrá un control de los servidores *browser* Internet/Intranet y se conseguirá una rápida implementación de los diferentes cambios y parches de los sistemas operativos.

Por otra parte estamos afrontando la creación de una red de expertos de seguridad en el nivel técnico (TISO), que permita una rápida respuesta a las vulnerabilidades e incidentes, a fin de que los BISO's puedan centrarse en la divulgación de las políticas, en la concienciación de usuarios y en conseguir que no se minusvalore la seguridad en los proyectos de negocio, utilizando donde sea posible la formación a través de web y cursos interactivos mediante nuevas herramientas de *e-learning*.

– En Citibank España se tratan por razones de negocio datos personales. ¿Ha sido especialmente compleja la adaptación al Reglamento? ¿Hay algún aspecto del Reglamento sobre el que ustedes hubieran agradecido mayor concreción a efectos técnicos?

– Desde la entrada en vigor de la LORTAD, en 1994, hemos estado atentos a su cumplimiento. Tenga en cuenta que por su estructura internacional Citibank ha estado muy afectado por esta legislación, al disponer de datos fuera de España, tanto en países de la UE como fuera de ella.

La adaptación reglamentaria, al ya tener implementadas desde hace años las medidas de seguridad de la corporación, que cubren de forma similar lo indicado en el Reglamento, no nos ha costado grandes esfuerzos. En su momento nos centramos especialmente en la descripción específica del Documento de Seguridad para ubicarlo en el contexto de los diferentes y amplios documentos y/o procedimientos ya en vigor en nuestra entidad, así como en la adecuación a la legislación vigente en materia de datos personales de los contratos y acuerdos de servicio con terceros.

En cuanto a complejidad puedo mencionar el borrado o bloqueo de los datos una vez finalizado su uso o por cualquier otro requerimiento, así como el mantenimiento de la calidad de los datos de morosidad, que al tener aplicaciones comunes que dan servicio a clientes de diferentes países, y la rigurosidad en materia de cumplimiento de fechas, nos ha llevado a extremar las precauciones.

Mención especial merece la realización de los documentos apropiados para el tratamiento de datos fuera del país así como en algunos casos fuera de la Unión Europea (EEUU, India, etc.), que ha requerido la elaboración por el área legal de los apropiados documentos que cubran debidamente las transferencias internacionales de datos o los acuerdos de servicio para la realización del soporte técnico remoto desde dichos países, cumpliendo la legislación comunitaria y local en materia de protección de datos, y las especificidades de cada país.

"Hay que evitar que para reducir el coste de un proyecto o sufrir retrasos en su finalización no se consideren, se ignoren o se dejen para segundas fases los aspectos de seguridad"

– ¿Tiene futuro profesional esto de la seguridad de la información?

– Desde la mitad de la década de los 80 en que empecé en las áreas de control y calidad dentro del área de Tecnología y realicé uno de los primeros Master en Auditoría Informática, y actualmente desde el terreno de la seguridad en el ámbito de negocio, no he visto ningún momento de retroceso en esta profesión. No obstante, en los últimos 5 años y posiblemente por los cambios legislativos y a remolque de los incidentes motivados por ataques de código malicioso y la aparición de nuevas vulnerabilidades en los sistemas, así como de los graves incidentes del 11-S, tanto las empresas como la administración y la propia industria de la tecnología y comunicaciones, dedican ya un buen porcentaje de su negocio a la protección de la información.

Desde la esfera profesional bien puede decirse que hay una demanda cada vez más frecuente de especialistas en seguridad de la información y, consecuentemente, se está generando una importante necesidad de formación, que debería verse reflejada también en el ámbito universitario. La industria de la seguridad informática es altamente cambiante, y sus expertos tienen que estar continuamente formándose. Cuando digo expertos no sólo me refiero a especialistas en tecnología, sino también a profesionales que puedan educar con ética a formar nuevos profesionales.

En Citigroup, vimos desde hace años la necesidad de disponer de especialistas bien formados a nivel técnico en seguridad de la información, así como en las áreas de control y auditoría, en privacidad de la información y en continuidad de negocio.

– ¿Qué aspectos de la gestión de los riesgos de seguridad TIC es el que le causa, profesionalmente, más quebraderos de cabeza?

– Van cambiando, aunque yo no los llamaría quebraderos de cabeza. En el año 2001 la palma se la llevó el control de los códigos maliciosos; el año pasado, la instalación rápida de los parches de las diferentes vulnerabilidades en los sistemas operativos. Actualmente, la principal preocupación se centra en la trasmisión y proceso de la información con terceros, sean proveedores o colaboradores, ámbito en el que hemos de aplicar medidas de seguridad y hacerles entender la necesidad de implementarlas en sus relaciones con nosotros, además de por la propia obligación que tienen de cumplir con la legislación sobre protección de datos.

Sí hay algo que yo calificaría de quebradero de cabeza continuo en una empresa como la nuestra, tan dinámica y con cambios permanentes en la gerencia y a otros niveles: hacer entender a los directores de negocio y jefes de proyectos la necesidad de adoptar e implementar las medidas de seguridad desde el inicio de cualquier proyecto a pesar de su posible repercusión en materia de presupuesto y tiempo. Obviamente, en algunos casos no se hace por necesidad sólo, sino por obligación.

Hay que evitar que para reducir el coste de un proyecto o sufrir retrasos en su finalización no se consideren, se ignoren o se dejen para segundas fases los aspectos de seguridad. ■

Texto: **José de la Peña Muñoz**
Fotografía: **Jesús A. de Lucas**