ARI

ARI 36/2014

16 de julio de 2014

Las embajadas de datos: la protección de la información estatal

THIBER - The Cybersecurity Think Tank.

Tema[1]

Este ARI analiza el concepto de "embajada de datos" como un nuevo instrumento de la política exterior para asegurar el funcionamiento de los servicios públicos esenciales frente a riesgos cibernéticos.

Resumen

Estonia está considerando la posibilidad de replicar fuera del país las bases de datos informáticas que permiten la prestación de servicios públicos esenciales para mitigar el daño de una posible agresión o pérdida. La progresiva mentalización de las sociedades y gobiernos frente a los riesgos del ciberespacio les está llevando a dotarse de nuevos instrumentos de ciberseguridad y ciberdefensa que hace poco parecían de ciencia ficción. El riesgo –ya factible– que corren las bases de datos públicas en el interior de los países está llevando a reforzar sus infraestructuras de tecnologías de la información y las comunicaciones, pero también a pensar en nuevos instrumentos como la replicación de esas bases en el exterior para diversificar los riesgos y potenciar la resiliencia frente a ellos. Este ARI estudia las "embajadas de datos" como opción de respuesta, la experiencia estoniana y la forma en la que se podrían articular si se consideran interesantes para la política exterior y la ciberseguridad de un país.

Análisis

Introducción

En la actualidad, las tecnologías de la información y de las comunicaciones (TIC) soportan el grueso de los servicios públicos de todos los países; desde la hacienda pública, la seguridad social, el censo, los servicios judiciales, la sanidad y la seguridad y defensa. Debido a su trascendencia, los países que disponen de mayor madurez tecnológica y que han analizado los riesgos asociados a una eventual pérdida de estos datos están ahora tomando medidas para evitar que el propio

1 Guillem Colom Piella, Enrique Fojón Chamorro, Adolfo Hernández Lorente, José Ramón Coz Fernández, Ángel Vallejo Chamorro, David Barrancos Larráyoz y José María García Alias forman parte del grupo de trabajo sobre "Embajadas de Datos" dirigido por THIBER, *The Cybersecurity Think Tank*.

Estado y los servicios básicos que se proporcionan a los ciudadanos dejen de funcionar. Algo parecido ocurre en el ámbito privado, donde muchas organizaciones, empresas y ciudadanos han puesto en marcha interesantes iniciativas para minimizar estos riesgos. Sin embargo, la responsabilidad última de la custodia de la información crítica para el funcionamiento de los países corresponde a los gobiernos, ya que los sistemas TIC y las bases de datos gubernamentales son parte de la soberanía del país, por lo que los poderes públicos deben preocuparse de adoptar las medidas de seguridad que mayores garantías ofrezcan.

Estonia ha ido un paso más allá en este proceso y está planteado replicar en el exterior la información y servicios esenciales para garantizar el normal funcionamiento del país en caso de conflicto o catástrofe. Su traslado al exterior tiene una función de copia de seguridad (*backup*) para que el gobierno pueda restablecer el funcionamiento de los servicios públicos básicos cuanto antes (*resiliencia*) y su réplica en las distintas embajadas reduciría enormemente la probabilidad y el impacto de un apagón total.

Estonia: paradigma de la e-nación

Esta pequeña república báltica ha encontrado en las nuevas tecnologías un pilar fundamental para su construcción nacional en la era de la información y del conocimiento. La situación geográfica y la realidad geopolítica del país, su pequeña población (apenas 1,3 millones de habitantes), la integración de su sistema administrativo y un conjunto de políticas inclusivas que han creado un entorno propicio para la integración política, social y económica a todos los niveles de la administración estonia han sido los elementos que han posibilitado esta evolución hacia convertirse en una *e-nación*.

La apuesta de Estonia por las nuevas tecnologías es imparable. Ha desarrollo una e-administración tan avanzada que permite a sus ciudadanos realizar todos los trámites necesarios para crear una empresa en tan solo 18 minutos y votar a través de Internet (2005) o del teléfono móvil (2008). En el aspecto económico ha fomentado la investigación y desarrollo de empresas como la archiconocida *Skype* o de centros tecnológicos como *Tehnopol*, formado por más de 150 empresas.

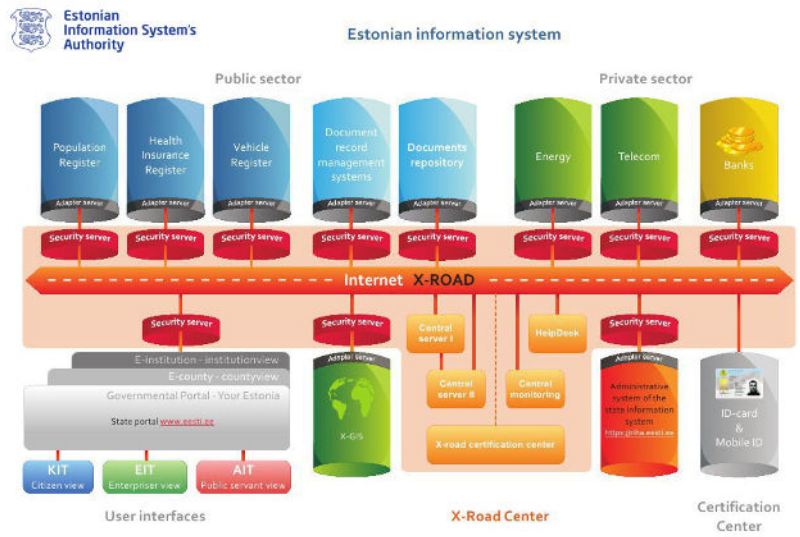
Sin embargo, esta misma interconectividad y nivel de apertura tecnológica que han permitido a Estonia crecer como país, también han incrementado sensiblemente su nivel de riesgo. Así, durante los meses de abril y mayo de 2007, muchos de los servicios *on-line* proporcionados por actores públicos y privados estonianos quedaron parcial o totalmente interrumpidos debido a un conjunto de ataques de denegación de servicios distribuidos (DDoS) supuestamente provenientes de Rusia. Éstos comenzaron cuando el ejecutivo estoniano trasladó desde el centro de Tallin a un cementerio situado en las afueras de la capital la estatua del Soldado de Bronce, un monumento erigido en honor a los militares soviéticos caídos combatiendo el nazismo pero que para muchos ciudadanos estonianos

representaba a quien durante medio siglo había ocupado el país. Durante estos ciberataques, y para preservar su soberanía, el gobierno de Tallin trató de aplicar a esta nueva amenaza la garantía del Artículo 5 del Tratado del Atlántico Norte diseñada para defender la soberanía de los Estados miembros ante un ataque armado. Desde entonces, y particularmente durante la Cumbre de Bucarest que se celebró un año después, los aliados han tratado de articular una respuesta colectiva frente a las nuevas amenazas cibernéticas. Pocos meses después, la OTAN estableció en Tallin su Centro de Excelencia Cooperativo en Ciberdefensa (CCD CoE en sus siglas inglesas) y, en 2010, el nuevo Concepto Estratégico de la Alianza Atlántica aprobado en Lisboa integró el factor cibernético en el catálogo de riesgos y amenazas a los que se podría enfrentar esta organización.

Recientemente, Jaan Priisalu, director de la Agencia de Sistemas de Información del gobierno estoniano, anunciaba la intención del ejecutivo del país de crear un conjunto de centros de datos repartidos en varios puntos del globo. Conocidos como “embajadas de datos”, se pretende que estos centros alberguen una réplica de los sistemas de información y los datos críticos necesarios para garantizar el funcionamiento del país en caso de contingencia. Estas infraestructuras se situarían en las capitales de sus principales aliados y socios, preferentemente en las embajadas localizadas en ellas si disponen del espacio físico y de los recursos tecnológicos necesarios para albergar estos centros de datos. En el caso de que no dispongan de las condiciones necesarias, sería necesario establecer embajadas de datos fuera de las instalaciones de las sedes diplomáticas estonias.

En la actualidad, la piedra angular de la administración electrónica estonia reside en el *X-Road*, una capa de intercambio seguro de datos a través de Internet entre los distintos sistemas TIC del país, tanto públicos (como los registros de población, sus datos sanitarios, fiscales o sociales, los registros de vehículos u otra información relevante para la administración del país) como privados (de las empresas proveedoras de energía, telecomunicaciones o el sistema bancario).

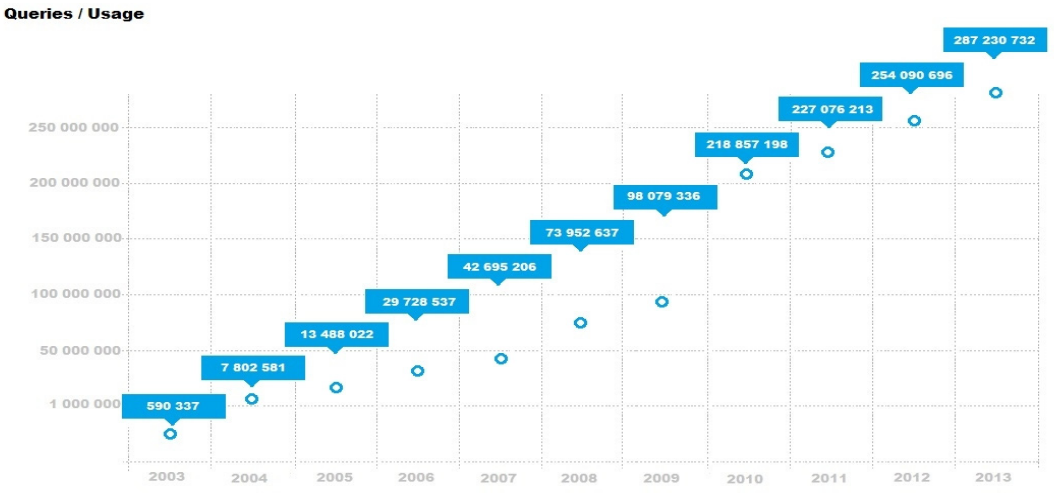
Figura 1. Arquitectura de *X-Road*



Fuente: Estonian Information System´s Authority (**https://www.ria.ee/en**).

Precisamente, el empleo del *X-Road* ha motivado un incremento exponencial de la interconexión entre los sistemas de información del país, puesto que no sólo se ha limitado a la administración pública sino también al sector privado. En la actualidad, cerca de 180 bases de datos gubernamentales y privadas están conectadas a este sistema, lo que permite la prestación de cerca de 2.000 servicios distintos por parte de 900 organizaciones estonias, tanto públicas como privadas.

Figura 2. Estadísticas de uso de *X-Road* (número de consultas/año)



Fuente: X-road (**www.x-road.eu**).

A pesar de este elevado nivel de madurez tecnológica en Estonia, Taavi Kotka –responsable de la seguridad de la información del gobierno– aboga por replicar y migrar los sistemas TIC y los datos críticos a las embajadas de datos como pilar fundamental de la futura "nube estatal estoniana" que contenga toda aquella

información gubernamental y privada necesaria para garantizar el correcto funcionamiento del país en caso de contingencia (invasión, ciberataque o desastre natural, entre otras).

Tras los sucesos de Ucrania, el gobierno estoniano ha acelerado sus planes para crear embajadas de datos alrededor del mundo. Para ello ha dividido la información del país en dos grupos: sensible y no-sensible:

- La información sensible se alojará en los centros de datos (*data centres*) de las embajadas de datos que se habiliten. Se pretende que estas instalaciones que albergarán copias de seguridad de todas las bases de datos sensibles del país se construyan en las capitales de sus principales aliados y amigos, entre los que se barajan el Reino Unido, Finlandia, los Países Bajos, EEUU y Japón.

- La información no-sensible se alojará en proveedores de servicio internacionales como Amazon, con los que el gobierno firmará exigentes acuerdos relativos a la disponibilidad y resiliencia de los sistemas que dan soporte a esta información.

La importancia estratégica de las embajadas de datos

Concebida para albergar información sensible (como pueden ser datos relativos al censo nacional, la seguridad social o la Administración del Estado, entre otros) de un país en el extranjero, la embajada de datos estará apoyada por otras bases de datos emplazadas en proveedores de servicios de Internet privados que podrán albergar toda aquella información no-sensible para el país.

Planteadas así, las embajadas de datos añaden una nueva variable a la compleja ecuación de la política exterior y suponen un reto para la seguridad y la defensa de muchos países de nuestro entorno. Sin embargo, la idea técnica que subyace tras estas embajadas de datos es menos novedosa de lo que podría pensarse en un primer momento. De hecho, son muchos los organismos y agencias gubernamentales que disponen de copias de seguridad de sus datos en otras localizaciones auxiliares situadas en el territorio nacional. De manera similar, muchas empresas y corporaciones también replican sus bases de datos en otras instalaciones localizadas tanto en el propio Estado como en terceros países. En ambos casos, tanto los gobiernos como las empresas también disponen de mecanismos de contingencia para operar su infraestructura TIC en caso de necesidad.

En consecuencia, lo que convierte a las embajadas de datos en algo revolucionario no es su vertiente técnica, puesto que el almacenamiento de información en servidores externos o en la “nube” es algo que se ha normalizado en los últimos años, sino que lo realmente novedoso es que sea un gobierno el que implemente esta solución, replicando buena parte de su información, incluida la sensible y clasificada, en diversas localizaciones físicas fuera del territorio nacional, bien sea

en terceros países dentro de instalaciones sujetas al derecho diplomático y consular o en servidores privados. Es una opción que se debe sopesar porque su réplica no está exenta de riesgos, tanto por aquellos relacionados con la inherente vulnerabilidad de las TIC como por la posibilidad de que la información sea replicada por el país que alberga la embajada de datos mediante el uso de tecnologías de ciberespionaje; además de que los condicionantes físicos, técnicos, económicos y políticos que conllevan dificultan su generalización.

El concepto de embajada de datos

Tal y como se ha expuesto, Estonia está trabajando activamente en la creación de embajadas de datos que permitan a Tallin gobernar desde la "nube" en el medio plazo. Sin embargo, tal y como ya se ha comentado, para llegar a este extremo es necesario disponer de un conjunto de elementos, siendo los más importantes el nivel de madurez de las TIC estatales y la existencia de entes administrativos con unas funciones concretas y limitado solapamiento.

En este sentido, todos los países deberían –en el corto o medio plazo– aspirar a crear embajadas de datos que permitan funcionar como centros de respaldo en los que se repliquen los sistemas de información y comunicaciones y las bases de datos críticas para el normal funcionamiento del Estado.

En sentido estricto, una embajada de datos es una instalación que está formada por un centro de datos y por un área de trabajo para la gestión y administración del centro de datos, que tiene como misión replicar los sistemas TIC y las bases de datos criticas de un Estado con el objeto de evitar que se pueda perder información o que sus operaciones criticas se vean interrumpidas como consecuencia de una amplia gama de contingencias.

El centro de datos de cada embajada de datos albergará información de titularidad pública y de carácter sensible o clasificado de un Estado que merezca su duplicación fuera del país. Se albergara preferentemente en infraestructuras nacionales en el exterior (desde embajadas físicas a buques con pabellón nacional), aunque también pueden albergarse otros lugares -incluyendo servidores privados- bajo convenio de colaboración y confidencialidad.

A la hora de establecer las embajadas de datos será necesario tener en cuenta, entre otros, los siguientes aspectos:

- En primer lugar, hay que definir criterios de selección para identificar qué datos sensibles pueden ser alojados en un proveedor de servicio externo y qué tipo de información puede replicarse en bases de datos privadas. En este sentido, mientras la información referente al censo, impuestos, firma electrónica, e-gobierno, registro de empresas, seguridad social o pensiones podría estar replicado en las embajadas de datos situadas en el exterior, la información relacionada con la seguridad y la defensa nacional no debería, *a priori*,

replicarse en estas instalaciones; y de hacerlo, solamente debería hacerse en las embajadas de datos principales bajo las mismas premisas en las que hoy en día esta información se comparte con organismos internacionales como la Alianza Atlántica, la UE o las Naciones Unidas, entre otros.

- En segundo lugar, hay que planificar y presupuestar la duplicación de datos, ya que los costes de la creación, adecuación y mantenimiento de una embajada de datos serán elevados, por lo que será fundamental establecer dónde se instalarán, cuántas se instalarán y qué información se replicará. Del mismo modo, hay que analizar el ritmo de crecimiento de las bases de datos a replicar, dado que el número de servicios críticos de un país dependiente del ciberespacio aumentará de manera exponencial, y con ello los requerimientos técnicos y funcionales de las embajadas de datos.

- Finalmente, y aunque las embajadas de datos sensibles se establezcan en países con los que se tengan muy buenas relaciones y gran confianza, sería necesario estudiar su régimen diplomático, para conocer los derechos y obligaciones que genera su establecimiento para cada parte, tanto dentro como fuera de las embajadas. Cuando las embajadas contengan datos no sensibles y se alberguen en instalaciones privadas de otro país, será necesario definir el régimen jurídico de su instalación en función de la legislación aplicable en cada país.

Propuestas para la articulación de las embajadas de datos

Las embajadas de datos podrán ser de tres tipos (principales, secundarias y externas) dependiendo de su funcionalidad, nivel de clasificación de la información que manejen y de su ubicación física.

- Las embajadas de datos principales serán centros de datos de respaldo en los que se realizará una copia síncrona[2] o asíncrona[3] dependiendo de las necesidades operativas y las capacidades tecnológicas de la información contenida en las principales bases de datos de titularidad pública y de carácter sensible o clasificado de un Estado. Estas embajadas dispondrán del mismo equipamiento electrónico e informático y la misma versión del *software* que los centros de datos principales del país con el objeto de evitar perdida de información o cese de operaciones criticas. Se ubicarán dentro de las representaciones diplomáticas nacionales situadas en los principales países socios o aliados y, solamente en caso de necesidad, en nuevas instalaciones con estatus diplomático.

2 Una copia síncrona es aquella que garantiza que todo dato escrito en el centro de datos de origen también se escribe en el centro de respaldo antes de continuar con cualquier otra operación.
3 Una copia asíncrona es aquella que no asegura que todos los datos escritos en el centro de datos de origen se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

- Las embajadas de datos secundarias serán centros de datos de respaldo donde se realizarán copias asíncronas de un número reducido de las principales bases de datos de titularidad pública y de carácter sensible de un Estado. Éstas dispondrán de un equipamiento electrónico e informático compatible y la misma versión del *software* que los centros de datos principales del país con el objeto de evitar cualquier pérdida de información o cese de operaciones. Al igual que las embajadas principales, éstas también estarían emplazadas dentro de las representaciones diplomáticas nacionales situadas en los principales países socios o aliados y, en caso de necesidad, en nuevas instalaciones que gozaran de estatus diplomático.

- Las embajadas de datos externas serán centros de datos que albergarán servicios y datos no-críticos del Estado. Éstas se encontrarán situadas en proveedores privados con los que los países habrán firmado un exigente acuerdo de nivel de servicios en los que se asegure la disponibilidad de la infraestructura de tecnologías de la información y las comunicaciones y la integridad y confidencialidad de los datos.

A la hora de establecer una embajada de datos, principal o secundaria, es necesario tener en cuenta la seguridad. Ya que ningún régimen jurídico por sí mismo garantiza las medidas de seguridad necesarias, será necesario implantar aquellos mecanismos, generalmente de prevención y detección, destinados a proteger el emplazamiento, la seguridad física perimetral y del centro de datos y el nivel de redundancia.[4] También es necesario disponer de las tecnologías de la información y las comunicaciones necesarias para garantizar la disponibilidad y resiliencia del mismo, así como asegurar la gestión, operación y gestión de incidentes. Una tecnología que precisa personal especializado y que cuente con las habilitaciones de seguridad preceptivas.

Conclusiones

A medida que nos adentramos en la era del conocimiento, nuestras sociedades están cada vez más interconectadas y las administraciones públicas manejan y cruzan cada vez mayores volúmenes de datos. Aunque éstos se hallan almacenados y replicados en múltiples servidores nacionales, países como Estonia –con un alto nivel de madurez tecnológico, altamente dependiente de las TIC, con una administración integrada y con una amenaza latente a pesar de su pertenencia a la Alianza Atlántica– han decidido ir un paso más allá e intentar replicar los servicios y los datos críticos del país en servidores nacionales en el exterior y los no-críticos en servidores de empresas privadas.

4 Planteada por ***Uptime Institute*** y plasmada en el estándar ANSI/TIA-942, el TIER de un centro de datos se refiere al nivel de redundancia de los componentes que soportan ese centro. A fecha de hoy, existen cuatro TIER, siendo el cuarto el más redundante, por lo que éste debiera ser el nivel de las embajadas principales, mientras que el de las secundarias podía ser de nivel 3.

Aunque no compartan las características descritas de Estonia, otros países deberían plantearse la posibilidad de construir embajadas de datos que contengan la información fundamental para garantizar el funcionamiento de la administración del Estado en caso de producirse cualquier tipo de crisis, conflicto o catástrofe.

Cada país debe evaluar la naturaleza y dimensión de los datos a proteger, los diferentes niveles de su Administración pública, sus estándares de información y su nivel de madurez tecnológica porque condicionan el establecimiento de embajadas de datos en el extranjero que repliquen los servicios públicos que afectan a la seguridad nacional.

La existencia de estas embajadas de datos puede servir como base sobre la cual gobernar desde la "nube", puesto que en un futuro cercano los sistemas y servicios básicos de un país podrían continuar funcionando desde ella a pesar de que se hubiera producido una catástrofe o crisis e incluso un ciberataque contra los sistemas nacionales. Sin embargo, ello también plantea nuevas preguntas y añade una nueva variable a la compleja ecuación de la política exterior. Y es que si bien las embajadas de datos situadas en las sedes diplomáticas del país mantendrán todas las prerrogativas y el estatus de esta misión, no es menos cierto que existe la posibilidad –tal y como ya se ha producido en varios casos con independencia de su ilegalidad– que toda la información transmitida a estos centros de datos sea también copiada por el país que alberga esta embajada. Es por ello que las embajadas de datos deberán plantearse en países aliados o amigos e intentar suscribir convenios adicionales, aunque ello no signifique –tal y como ha demostrado el escándalo Snowden– que no realicen labores de espionaje. Igualmente, aunque la información situada en servidores privados en ningún caso será vital, ya que con independencia de los convenios firmados con empresas privadas no puede descartarse que toda la información pueda ser comercializada o utilizada para otros fines no legítimos.