EN ESTE TIEMPO DE REFORMAS...TRANSFORMACIÓN DE LA ADMINISTRACIÓN IMPULSADA DESDE LAS TIC Y RETOS DE CONTINUIDAD DEL NEGOCIO

¿Seguro que la virtud está en la prudencia?

Dado que el uso de las tecnologías es algo cotidiano en nuestros días no debería tratarse ya de Administración Electrónica como algo distinto de la Administración, de igual modo que parece obsoleto hablar de internet o movilidad como si se tratasen de "nuevas" tecnologías. Pero bien es cierto que un uso adecuado de las tecnologías de la información puede ser clave para lograr la modernización o transformación interna de la Administración, con el objetivo de incrementar la productividad y reducir los costes de prestación de servicios. Este propósito vuelve a aparecer en la Agenda Digital para España, a través del objetivo de mejora de la eficiencia de los servicios públicos mediante el uso de herramientas digitales, para contribuir a la recuperación económica.

POR ROCÍO MONTALBÁN CARRASCO

El rápido desarrollo de las TIC y su incremental uso en el sector público, privado y residencial está teniendo un importante impacto que alcanza todos los ámbitos de la economía y la sociedad. Mientras que el crecimiento del PIB en España está estancado desde el cuarto trimestre del año 2008 **(1)** , y el IPC acumulado se encuentra alrededor de los 8 puntos porcentuales, el sector de las telecomunicaciones y las tecnologías de la información parece ajeno a estas turbulencias macroeconómicas, siendo una de las pocas industrias con crecimiento en los últimos años, situándose su inflación con valores negativos y muy por debajo del índice general del IPC.

La actual demanda de productos »

y servicios tecnológicos desafía casi cualquier indicador de crecimiento. La alta penetración de la banda ancha fija y móvil en España, con seis de cada diez hogares conectados a internet y 32,4 millones de usuarios móviles **(2)** y el uso de las redes sociales, han provocado grandes cambios en las relaciones humanas, en la sociedad en general y en el mundo corporativo, tal como muestran los siguientes datos:

- 16 millones de usuarios en Facebook **(3)** y 10 millones de usuarios de Tuenti en España.
- 27,9% de los usuarios móviles en España acceden a través de conexiones de banda ancha.
- 4700 mensajes de texto enviados por un adolescente medio/mes **(4)**.
- Más de 40 proyectos en curso de ciudades inteligentes en España **(5)**.

En relación a la Administración Electrónica, España cuenta con 23,2 millones de internautas, de los cuales el 31 % utilizan la red para relacionarse con la Administración y, por supuesto, quieren hacerlo de modo similar al que utilizan para disfrutar de otros servicios: a través de cualquier dispositivo conectado a la red, de forma sencilla y con garantías de seguridad.

Derecho de acceso

Pero no sólo los ciudadanos y empresas requieren el uso de las tecnologías como derecho de acceso a la Administración Pública por medios electrónicos, sino que internamente se deben asentar las TIC como parte de la actividad administrativa. Según el Foro Económico Mundial, los países que encabezan la lista en cuanto a crecimiento económico y competitividad coinciden con aquellos que más destacan en apertura y eficiencia del sector público y en preparación para la e-Administración. Además, esta transformación está cambiando la forma de operar de las compañías de todo el mundo para reducir sus costes de operación y permitir mayor flexibilidad. Los negocios de hoy implican el uso constante de la información y el acceso al conocimiento de las organizaciones como parte de sus procesos de trabajo. Cada vez más, la información contribuye a la creación de valor añadido de la mayoría de productos. Por eso, las herramientas de colaboración, como el correo electrónico y las redes sociales, y la conectividad mediante dispositivos móviles a aplicaciones y datos descargables, a través de Internet, son necesarias para desarrollar la actividad en las organizaciones. La disponibilidad del acceso a estos servicios resulta crítica para asegurar la continuidad del negocio. Implica la necesidad de escalarlos, securizarlos y monitorizarlos como instrumentos que permiten recibir o enviar información (en especial la mensajería, la navegación y las herramientas de colaboración).

En general, se puede afirmar que el término trabajo ya ha dejado de representar un sitio físico (la oficina) para convertirse en una actividad (negocio), hasta el punto de que una de las piezas más importantes de la ubicación en la que se desarrolla es la disponibilidad en ese lugar de conexión a Internet, de modo que sea posible relacionarse con proveedores, compañeros y clientes y acceder a información. Si en la oficina fallase esta conexión, cualquiera entendería que el trabajador tuviera que irse a casa para continuar trabajando. Igualmente, sería inadmisible el hecho de que la ventanilla electrónica de la Administración no estuviera abierta a la solicitud de un ciudadano, o que el nivel de respuesta fuese inferior o menos riguroso.

Es, por tanto, necesario aprovechar las oportunidades que ofrecen las redes colaborativas y las TIC para transformar la prestación de servicios públicos en consonancia con la realidad actual, con un mayor intercambio e interacción con los ciudadanos en aras de lograr más productividad.

Nuevos retos

Esto reta a los profesionales TIC a encontrar el punto de equilibrio entre la demanda de inmediatez, ubicuidad, transparencia y colaboración y los riesgos derivados de la mayor exposición de datos internos de la organización, de datos personales, ante la existencia de accesos por múltiples puertas virtuales a las redes y aplicaciones, y ante la existencia de cadenas de proveedores de propietarios de la información, gestores y operadores, potenciado todo ello por la frontera difusa entre información privada y corporativa.

El cloud computing, como tendencia natural a soportar las soluciones tecnológicas adecuadas para esta forma de relacionarse, está provocando un cambio en la forma de salvaguardar los datos de negocio. Se mantienen las principales líneas de actuación en cuanto a la necesidad de identificar los procesos y la información crítica de negocio que debe protegerse, de evaluar económicamente el coste de un incidente de continuidad para diseñar salvaguardas o planes de recuperación proporcionales y la necesidad de implicar a la organización en la definición y aprobación de la estrategia de seguridad. Pero se pasa de un modelo de seguridad física y lógica interno en los centros de proceso propios, hacia modelos en los que son otros los que se ocupan

de esta custodia, recordando, con sus salvedades, al sistema de custodia de objetos de valor y depósitos monetarios en los bancos. Nadie duda hoy en día de que los mecanismos de vigilancia instalados en los bancos son muy superiores a los que pueden permitirse los particulares, incluso para aquellos que disponen de cajas fuertes y seguridad privada en sus domicilios. Aunque, bien es cierto, que esta confianza de los ahorradores no se consiguió de un día para otro, sino que fue necesario un proceso regulador y de control y un proceso de aceptación por parte de la sociedad. Y aun así, la forma de relacionarse con los bancos para retirar dinero (siguiendo el paralelismo de los ahorros depositados con la información en el cloud computing) ha ido cambiando gracias a la tecnología y a la necesidad de cubrir una demanda de uso, que iba desde la disposición a través de ventanilla, las tarjetas de crédito, los cajeros automáticos, la banca telefónica y por internet, etc.

En esa línea, también es cierto que hasta que no hemos tenido unas redes de comunicaciones de alta velocidad y fiabilidad, resultaba más operativo tener los datos cerca de las empresas, igual que mientras no había cajeros y tarjetas de crédito necesitábamos disponer de más efectivo. Pero hoy que la tecnología y los hábitos de consumo apuntan al acceso en remoto de la información, las nubes públicas o privadas, con una agregación de servicios TIC y unos especialistas profesionales que las exploten, permiten altas garantías de seguridad, con un coste/unidad muy ajustado.

Otra corriente favorecida en muchas empresas, y a la que no escapa la Administración Pública, es el uso de múltiples dispositivos móviles personales en entornos corporativos y viceversa, haciéndose cada vez más difusa la frontera entre el uso laboral y particular. Se conoce por las siglas BYOD (Bring Your Own Device) y va en consonancia con la mayor movilidad y flexibilidad demandada por los trabajadores, que esperan que los responsables de Tecnologías de la Información les permitan utilizar cualquier terminal para acceder a la intranet corporativa. Esta práctica comienza a ser la norma más allá de excepciones. Para ello, es necesario adaptar la capacidad de las aplicaciones e infraestructuras a esta nueva realidad. Una nueva ficha hacia el incremento de productividad laboral y un nuevo reto para garantizar la seguridad de la información teniendo en cuenta las soluciones de almacenamiento en red, comunicaciones unificadas, gestión de perfiles en redes sociales y la necesidad de dimensionamiento de accesos ina- »

lámbricos. Ello implica una mayor complejidad en la gestión en cuanto a la falta de estandarización y a la necesidad de acotar el ámbito del servicio técnico prestado. Cada una de estas iniciativas debe plantearse con un enfoque de compromiso entre la rentabilidad económica del proyecto y la garantía de seguridad y fiabilidad del tratamiento de los datos.

Exigencias de la nueva realidad

Los planes de seguridad tienen que renovarse y ajustarse para contemplar estas formas de organización del trabajo. La información fluye por muchos canales y en cada uno surgen unos riesgos que hay que gestionar para que no se interrumpa la actividad. La disponibilidad permanente de dichos canales se ha convertido en el punto de salida y no en la meta a lograr y se trata de manejar otra serie de amenazas más sofisticadas. La disponibilidad de los accesos inalámbricos, la virtualización con gestión de recursos para alta disponibilidad y el control de acceso a la red corporativa se han convertido en aspectos claves. Prima la prevención y la respuesta a incidentes con un enfoque que combina la *componente técnica y la organizativa*, desplazándose el peso de la balanza cada vez más hacia esta última, dada la dispersión en la propiedad, gestión y operación de los recursos.

La colaboración y *coordinación entre las entidades implicadas en el proceso para la prestación de servicios es clave para recuperación de desastres y continuidad del negocio*. Esto demuestra la necesidad de medidas para controlar y restringir el acceso lógico a datos, según el principio de mínimo privilegio necesario para cada función. En cuanto a la dispersión de dispositivos de acceso, cobra más importancia la protección de terminales móviles y tabletas con contraseñas de acceso, la encriptación de la información y el uso de plataformas de gestión remota de dispositivos para actuar en caso de robo o pérdida. En relación a la prestación de servicios de computación en la nube, debe *examinarse el plan de continuidad de negocio con la cadena de suministro de los servicios*. Ésta ofrece, potencialmente, mayor grado de disponibilidad una vez alcanzada una masa crítica que permita beneficios de calidad de servicio a menor coste, pero exige nuevos métodos de evaluación y gestión de riesgos. Deben evaluarse las *interdependencias* entre servicios prestados internamente y a través de nubes públicas o privadas y los controles disponibles en cada uno de los modelos, para medir posibles fallos en cascada y los planes de actuación como parte de la recuperación ante desastres. Todo ello debe estar definido, de forma rigurosa, en los acuerdos de nivel de servicio firmados, así como las métricas para evaluar su cumplimiento y penalizaciones, de modo que el *riesgo sea compartido con el proveedor de servicio*.

A principios de 2012 el gobierno americano lanzó un Programa Federal de Gestión de Riesgo y Autorización (FedRAMP) **(6)** para normalizar la forma de garantizar la seguridad con modelos de provisión en la nube. En esta misma línea, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) **(7)** ha hecho pública la Guía práctica "Procure Secure" para dotar de herramientas y metodologías que faciliten la definición de requisitos, así como la monitorización y el seguimiento de la seguridad de la información asociada a los servicios de computación en nube, proponiendo parámetros como: disponibilidad del servicio, respuesta a incidentes, gestión del ciclo de vida de la información, cumplimiento de estándares y gestión de vulnerabilidades o la gestión de registros y análisis forenses. La propia Agenda Digital para España, en su área de actuación de "Privacidad, Confianza y Seguridad" esperamos que atienda estas necesidades, de igual manera que se ha anunciado dentro de la Agenda Digital Europea, que trabaja para publicar un marco común o Estrategia Europea para la Seguridad en Internet.

NOTAS

1. INE: http://www.ine.es/varipc/index.do
2. ONTSI. Indicadores destacados de la Sociedad de la Información en España (abril 2012): http://www.ontsi.red.es/ontsi/sites/default/files/indicadores_destacados_si_abril_2012.pdf
3. Facebook: http://www.facebook.com/
4. Gartner. The top 10 strategic technology trends for 2012
5. Telefónica. Informe de la Sociedad de la Información en España
6. FEDRAMP: http://www.gsa.gov/portal/category/102371
7. ENISA: http://www.enisa.europa.eu/

Rocío Montalbán Carrasco
Subdirectora General Adjunta
de Tecnologías de la Información
y las Comunicaciones
Ministerio de Industria, Energía y Turismo