ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

18/2015 11 de febrero de 2015

*Jesús Gómez Ruedas**

ADIÓS A WINDOWS XP EN EL MINISTERIO DE DEFENSA: LECCIONES APRENDIDAS

ADIÓS A WINDOWS XP EN EL MINISTERIO DE DEFENSA: LECCIONES APRENDIDAS

Resumen:

El Sistema Operativo Windows XP ha sido uno de los protagonistas de este año 2014. Masivamente implantado en organizaciones profesionales de todo el mundo, la finalización del soporte por parte de su fabricante, Microsoft Corporation, ha supuesto una incidencia de alto impacto en muchas de esas corporaciones. El problema revestía un especial calado por el abanico de amenazas que se abría para la información corporativa en el caso de no realizar actuaciones de migración a otro sistema operativo actualmente gestionado por su fabricante. Aunque el fin del soporte ya había sido anunciado por Microsoft con varios años de antelación, restricciones económicas y de otro tipo han dificultado la gestión del cambio necesaria ante un desafío de esta naturaleza. El documento analiza algunas de las áreas de actuación que esconden herramientas para afrontar transformaciones de este tipo.

Abstract:

The Operating System Windows XP has been one of the stars in year 2014. Massively introduced in professional organizations throughout the world, the end of support from its manufacturer, Microsoft Corporation, has made a high impact incident for many of these corporations. The problem was of particular depth by the range of threats that opened for corporate information in the case of not doing anything for migration to another operating system currently managed by its manufacturer. Although the end of support had already been announced by Microsoft several years in advance, economic and other constraints have hindered the necessary change management facing a challenge of this nature. The paper analyzes some of the areas of acting that contain tools to address such transformations.

Palabras clave:

Windows; Defensa; riesgos; ciclo de vida de soporte; Seguridad de la Información; Microsoft; Tecnologías de la Información; amenazas; vulnerabilidades; sistema operativo; gestión por procesos; plan de migración; gestión del cambio; gestión de activos; gestión de la configuración.

Keywords:

Windows; Defense; risks; support life cycle; Information Security; Microsoft; Information Technology; threats; vulnerabilities; operating system; process management; migration plan; change management; asset management; configuration management.

Jesús Gómez Ruedas

Entre los días 21 y 23 del pasado mes de octubre la Jefatura de Sistemas de Información, Telecomunicaciones y Asistencia Técnica del Ejército de Tierra celebró en la monumental y extraordinaria ciudad de Cáceres la cuarta edición de sus Jornadas SICIS: Tres días para el debate y la reflexión acerca de los planes, proyectos, sistemas de información, operaciones militares, contratos, productos, seguridad de la información y otros recursos y capacidades relacionados con las Tecnologías de la Información en el ámbito del Ejército de Tierra y, en parte, del Ministerio de Defensa.

La mesa redonda titulada "Windows 7 y Windows 2008 Server. Experiencias y lecciones aprendidas" celebrada en la tarde de la primera jornada hizo emerger algunas cuestiones y preguntas que bien pueden servir de guía para recorrer la senda del aprendizaje sobre este nuevo caso de "efecto 2000[1]" acaecido en plena era del conocimiento.

ACTO PRIMERO: TIEMPO DE VERANO

Con toda seguridad, cualquier lector conservará entre sus recuerdos de la época escolar la fábula "La cigarra y la hormiga", atribuida al escritor griego Esopo y recreada tanto por el novelista francés Jean de la Fontaine como por el español Félix María Samaniego; en ella se podrían encontrar algunas similitudes con este capítulo contemporáneo de la joven y trepidante historia de las Tecnologías de la Información. Coincidencias, claro está, en lo que respecta al origen y el desarrollo de la trama, no en cuanto a la predisposición, voluntad o concepción del problema por parte de los protagonistas de esta moderna versión de la fábula que, con toda seguridad, no han actuado como la cigarra.

Como señalaba el Centro Criptológico Nacional en su Informe de Amenazas CCN-CERT IA-02/14 "Riesgos de uso de Windows XP tras el fin de soporte", ya en el año 2002 Microsoft había presentado su política de Ciclo de Vida de Soporte[2] con la finalidad de ofrecer transparencia y previsibilidad a la hora de comunicar y explicar las opciones de soporte de sus productos. De acuerdo a dicha política, los productos para empresa y desarrolladores, incluidos los sistemas operativos Windows y el paquete ofimático Microsoft Office, dispondrían de un mínimo de 10 años de soporte: cinco años de soporte estándar y cinco años de soporte extendido.

[1] Efecto 2000: Error de software causado por la costumbre que habían adoptado los programadores de omitir la centena del año para el almacenamiento de fechas (generalmente, para ahorrar memoria), asumiendo que ese software solo funcionaría durante los años del siglo XX cuyas primeras cifras fueran 19, dando lugar a eventuales riesgos de colapso de las aplicaciones al llegar el año 2000.

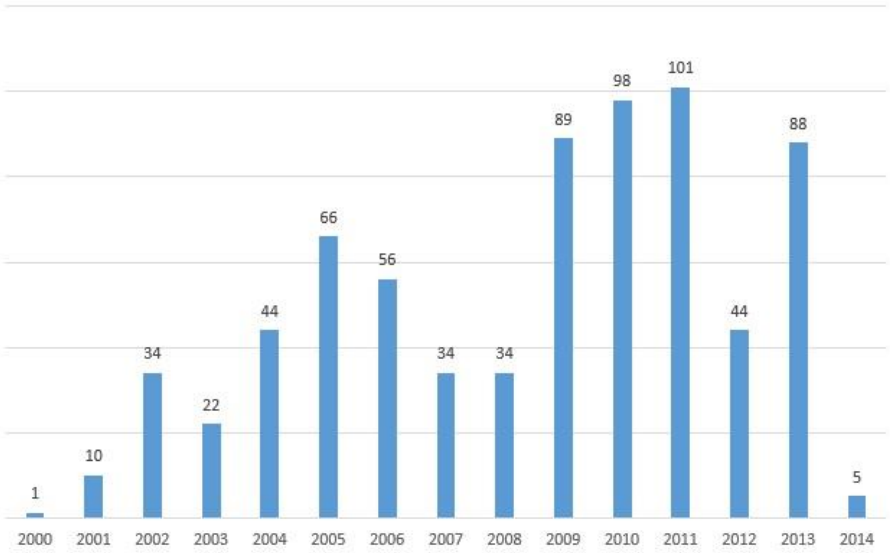
[2] http://windows.microsoft.com/es-es/windows/lifecycle

Unos meses antes, el 25 de octubre de 2001, se había presentado en los escritorios de ordenadores de todo el mundo el universal fondo de pantalla de un campo de Napa, California, propio de Windows XP, para dar el relevo al exitoso Windows 2000 y al no tan célebre ni reconocido Windows Millenium Edition (Me), proponiendo un sistema operativo unificado para el entorno empresarial y para el ámbito personal.

Aunque Windows XP había supuesto un giro copernicano de Microsoft en materia de seguridad, su dilatada hoja de servicios estuvo jalonada por tres actualizaciones "Service Pack" y por frecuentes y cruentos episodios en la lucha contra el malware: entre otros muchos, el gusano Blaster, en el año 2003; el gusano Sasser, en 2004; el gusano Conficker, en 2008; o las vulnerabilidades relacionadas con la funcionalidad "autorun" en 2011 y 2012. Poco a poco fue ganando la confianza de los usuarios[3], llegando a conquistar hasta el 95% de los escritorios de todo el mundo. Y mientras la edad y la sociedad contemporáneas iban incorporando nuevos "apellidos" (electrónica, de la información, digital, ciber, del conocimiento,…), las amenazas y los riesgos asociados a las Tecnologías de la Información se multiplicaban por doquier y, consecuentemente, el campo de Napa veía como las canas hacían palidecer los vivos colores de la verde colina y el azul cielo californianos: consideraciones comerciales al margen, resulta completamente natural que un sistema operativo diseñado y desarrollado en el ocaso del pasado siglo, entre diciembre de 1999 y agosto de 2001, encontrara, más de diez años después, serios y crecientes obstáculos para hacer frente a las modernas amenazas de un universo digital caracterizado por una hostilidad y beligerancia incrementales; solo hace falta echar un vistazo a la evolución de las vulnerabilidades identificadas en este sistema operativo para comprender la continua dificultad de mantenerlo seguro y a salvo de

[3] **Usuario** (ITIL 2011): Es una persona que utiliza los servicios de Tecnología de la Información en el día a día. Los usuarios son distintos de los clientes, ya que algunos clientes no utilizan el servicio de Tecnología de la Información directamente.

cada nueva vulnerabilidad descubierta que canalizara otro inédito vector de penetración de los últimos ejemplares de malware.



Evolución de las vulnerabilidades parcheadas anualmente en Windows XP (fuente Kaspersky Lab)

Coincidiendo en el tiempo con el nacimiento y crecimiento de Windows XP, la primera década del siglo había contemplado la consolidación de modelos metodológicos y marcos de buenas prácticas orientados a la gestión de unas infraestructuras corporativas de Tecnologías de la Información cuyo rápido crecimiento las había convertido en el bíblico "dragón de siete cabezas": Desde el paradigma de la gestión por procesos, marcos universales como ITIL, COBIT, ISO 20000 o ISO 27000 impulsaban el establecimiento de sistemas de gestión de la calidad que permitieran la gestión integral de los activos, del ciclo de vida de los servicios, de su configuración, de los permanentes cambios en los mismos, de sus requisitos de seguridad de la información, de sus costes, del control de los requerimientos de los clientes[4], de las relaciones con los suministradores, etc.; en definitiva, de mantener un adecuado dimensionamiento y control del empleo de las Tecnologías de la Información y, esencialmente, siempre alineado con las actividades y planes de negocio de la organización.

Y LLEGÓ EL INVIERNO

En junio de 2008 Microsoft anunciaba el fin de la distribución de Windows XP, aunque su soporte continuaría durante años hasta el pasado 8 de abril de 2014 en que, como sugería el reconocido

[4] **Cliente** (ISO/IEC 20000): Organización o parte de una organización que recibe uno varios servicios. Un cliente puede ser interno o externo a la organización del Proveedor del Servicio.

experto Chema Alonso, se convertía en "Abandonware[5]". Con antelación a este nuevo día D no solo el propio fabricante, sino todo tipo de organizaciones y profesionales de la comunidad de Seguridad de la Información, alertaban de la necesidad diseñar y ejecutar proyectos de migración que permitiesen erradicar el problema, de dimensión proporcional al tamaño de la organización y al número de sus estaciones de trabajo.

Desde ese día Microsoft no prestaría soporte de ningún tipo para este sistema operativo, es decir, ni actualizaciones de seguridad ni parches de resolución de incidencias. En consecuencia, el sistema operativo se erigía en una amenaza para los sistemas y aplicaciones corporativos y, por tanto, para la información de la organización. Una simple muestra de la lista de riesgos inherentes al uso de Windows XP resultaba tan extensa como preocupante:

- Windows XP se convertiría en un blanco fácil para explotar vulnerabilidades: una vez finalizada la publicación de actualizaciones de seguridad por parte de Microsoft, los atacantes y creadores de código dañino podrían centrarse especialmente en los sistemas XP.
- Cualquier red corporativa con una sola estación de trabajo Windows XP se encontraría en situación de riesgo. Una vez comprometido cualquier equipo XP, podría ser utilizado como trampolín para infectar al resto de equipos, independientemente de la tecnología de su sistema operativo.
- Seguiría existiendo un apreciable número de vulnerabilidades conocidas y no parcheadas. Así mismo, se estimaba que emergería también un importante número de vulnerabilidades aún no difundidas (de día cero).
- El mero hecho de mantener actualizados los antivirus comerciales no sería suficiente y, además, existía la posibilidad de que los fabricantes de software antivirus dejaran de actualizar sus soluciones para Windows XP.
- Un usuario interno malintencionado podría saltarse las protecciones implementadas por los administradores de la red y realizar actividades no autorizadas.

[5] **Abandonware**: Término informal compuesto de los vocablos en lengua inglesa "abandoned" y "software".

- Sin las actualizaciones de seguridad, las estaciones de trabajo de organizaciones privadas y públicas incrementarían el riesgo de incumplimiento de los requisitos legales que a cada una le pudiera resultar de aplicación: protección de datos de carácter personal, regulaciones en materia de sanidad, Esquema Nacional de Seguridad, marcos gubernamentales de Ciberseguridad, marcos reguladores de activos bancarios, etc.
- En los entornos de Seguridad y Defensa con manejo de información con algún nivel de clasificación, implicaría la pérdida de la correspondiente acreditación de seguridad para tratar dicha información.

Como si de un personaje más de la fábula se tratara, años después una plaga de filoxera atacaba los californianos campos de Napa donde se tomara la fotografía del fondo de pantalla del escritorio de Windows XP, llevándose parte de su belleza: ¡Tal vez fuera una consecuencia más del fin del soporte!

EN EL HORMIGUERO DE LA ADMINISTRACIÓN PÚBLICA

Más allá de las peculiaridades y restringida flexibilidad que supone la Ley de Contratos del Sector Público, en las Administraciones Públicas el escenario no era distinto, aunque para aquellos ministerios, como el de Defensa, con un volumen de usuarios rondando el centenar de miles de usuarios la situación tomaba tintes dramáticos: en organizaciones de estas dimensiones, el correspondiente plan de migración no se solventaba, simplemente, en el reducido plazo de unos pocos meses por medio de una serie de adquisiciones.

Con anterioridad al citado 8 de abril, la entonces recién creada Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de la Presidencia (actualmente encuadrada en el Ministerio de Hacienda y Administraciones Públicas) alcanzaba con Microsoft un Acuerdo de Soporte Personalizado de Windows XP para el conjunto de la Administración General del Estado que, con una duración de un año, permitía mitigar temporalmente los problemas económicos derivados de las adquisiciones de estaciones de trabajo y licencias del nuevo sistema operativo. Así pues, el día D se dilataba 365 días para el conjunto de los departamentos ministeriales. Simultáneamente se aceleraban los procesos administrativos de contratación del considerable parque de estaciones de trabajo que, por su antigüedad, necesitaban ser renovadas.

En el ámbito específico del Ministerio de Defensa, la anterior era una más de las medidas contempladas en el "Plan de actuación fin de soporte Windows XP en el Ministerio de Defensa" elaborado por la Subdirección General de Tecnologías de la Información y las Comunicaciones. Otras medidas de índole técnico consideradas en dicho plan giraban alrededor de actuaciones relacionadas con la completa normalización de equipos en el marco del dominio corporativo de Microsoft, los derechos de administración de la estación de trabajo, la gestión de los accesos de medios extraíbles de almacenamiento o el acceso a internet.

REFORMAS EN EL HORMIGUERO

Del mismo modo que la renovación del añejo tendido eléctrico o de las viejas tuberías de materiales obsoletos de una vivienda usada implican la realización de obras que afectan sobremanera a un gran número de dispositivos asociados o conectados y, también, impactan durante cierto periodo de tiempo a los servicios y la comodidad de sus inquilinos, la actualización del sistema de operativo de base de las estaciones de trabajo de una organización de cien mil usuarios y centenares de aplicaciones puede equipararse a un "Cambio Normal Complejo" o de alto impacto del indispensable proceso de Gestión del Cambio que, enmarcado en el correspondiente Sistema de Gestión del Servicio[6], constituye una herramienta imprescindible para cualquier Proveedor de Servicios[7] de Tecnologías de la Información. Al igual que esas reformas caseras, la dificultad implícita a este tipo de grandes despliegues no es una coartada para dejar de realizarlos.

Un Sistema de Gestión del Servicio corporativo razonablemente maduro constituye el complemento indispensable para que la inversión de los imprescindibles recursos económicos que se precisan en este tipo de proyectos de cambio proporcione los beneficios esperados.

[6] **Sistema de Gestión del Servicio** (ISO/IEC 20000): Sistema de Gestión para dirigir y controlar las actividades de gestión de los servicios del Proveedor del Servicio. Incluye todas las políticas de gestión del servicio, objetivos, planes, procesos, documentación y recursos requeridos para el diseño, transición, provisión y mejora de los servicios para el cumplimiento de los requisitos de esta parte de la Norma ISO/IEC 20000.

[7] **Proveedor del Servicio** (ISO/IEC 20000): Organización o parte de una organización que gestiona y provee uno o varios servicios al cliente. Un cliente puede ser interno o externo a la organización del Proveedor del Servicio.

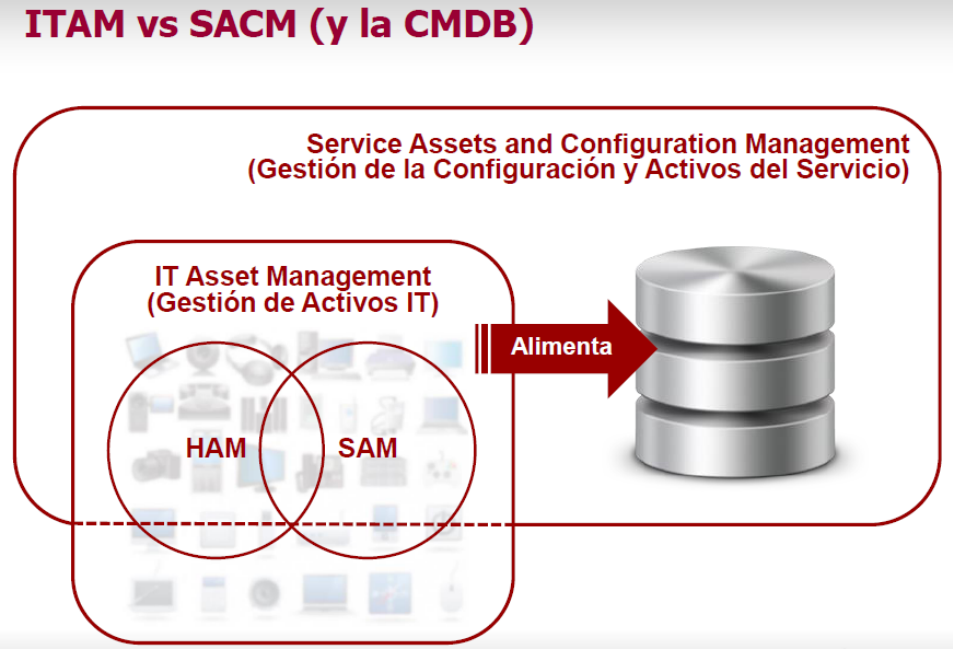
Cuando la madurez de los procesos propios del Sistema de Gestión del Servicio es moderada, el combate adquiere rasgos de heroísmo, pero la victoria sigue siendo posible:

- Sin un proceso de Gestión de Activos que, soportado fundamentalmente por herramientas de descubrimiento automático y de inventario de activos, registre y gestione el ciclo de vida de cada uno de ellos en la correspondiente Base de Datos, resultará de infinita complejidad conocer la cifra y estado real de esos activos. Pero un mero inventario técnico carente de datos económico-financieros y administrativos no es Gestión de Activos; cuando los repositorios de datos son diversos y diseñados con diferentes criterios, tampoco se tiene Gestión de Activos; si solo se consideran los activos de hardware y se presta menos atención a los activos software (licencias) y los contratos, no hay Gestión de Activos;…
- Sin el imprescindible proceso de Gestión de la Configuración no será posible conocer en qué servicios se encuadran los diferentes componentes de la infraestructura y de la organización identificados como Elementos de Configuración[8]. Lógicamente, es indispensable que el proceso sea soportado por una Base de Datos de Gestión de la Configuración (CMDB) adecuadamente asociada o integrada con las herramientas de descubrimiento automático e inventario de activos.
- Sin el correspondiente proceso de Gestión del Cambio que habilite la planificación, ejecución, control y mejora del ciclo de vida de todos los cambios realizados en los servicios de

[8] **Elemento de Configuración** (ISO/IEC 20000): Elemento que es necesario controlar para proveer uno o varios servicios.

Tecnologías de la Información, será imposible disponer en tiempo real de los datos e información que permitan la toma de decisiones, en particular de aquellas relacionadas con los costes, los presupuestos y las futuras adquisiciones.

A la hora de afrontar el problema deben diferenciarse los conceptos de Activo y de Elemento de Configuración: Un **activo** es cualquier elemento tangible del que interesa mantener un inventario y un control económico-financiero; un **Elemento de Configuración** es cualquier elemento, no necesariamente tangible, relevante para la prestación de un servicio de Tecnologías de la Información de cuya configuración debe mantenerse información actualizada. Por lo tanto, la atención de la Gestión de Activos se concentra en el control absoluto de la infraestructura, visión tecnológica, mientras que la Gestión de la Configuración se focaliza en los servicios del Catálogo de Servicios del Proveedor de Servicios, es decir, con orientación a los procesos funcionales de negocio. De forma simplificada, y al margen del diseño de las bases de datos donde se almacenen los datos de activos y Elementos de Configuración, los datos de la Gestión de Activos constituirán en buena parte un subconjunto de la Base de Datos de Gestión de la Configuración (CMDB):



Integración de Gestión de Configuración y Activos del Servicio y Gestión de Activos (fuente ProactivaNET)

La Gestión de Activos proporciona un inventario completo de los activos desde el momento de adquisición hasta su salida del entorno de operación. Así pues, cuando los procesos de adquisición se multiplican por parte de diferentes actores, la información se atomiza y pierde integridad, las responsabilidades acerca del resto del ciclo de vida del activo también se difuminan y el rol del Proveedor del Servicio y el propio Sistema de Gestión del Servicio adquieren inconsistencias, puesto que aquél no dispone de la autoridad adecuada, ni de los datos precisos y necesarios para elevar las

pertinentes propuestas de adquisiciones o renovaciones de activos al órgano corporativo responsable de las gobernanza de las Tecnologías de la Información. En consecuencia, la participación simultánea en un mismo proceso de gestión de diversos actores con un rol idéntico o semejante de "Alto Responsable" (Accountable) de la matriz RACI[9] y sobre un conjunto de activos que forman parte de una infraestructura común conlleva el riesgo de pérdida de eficacia y merma de eficiencia.

Precisamente, el sistema operativo de las estaciones de trabajo de una red corporativa es una de las entidades manejada dentro del proceso de Gestión de Activos. El proyecto de despliegue del mismo en una organización de grandes dimensiones requiere de una estrategia de gestión integral de los activos corporativos y de la configuración de los servicios que debe estar soportada por herramientas automatizadas: Aunque de naturaleza y finalidad distinta, los Activos y los Elementos de Configuración están estrechamente vinculados y participan de una cadena de suministro de los Servicios de Tecnologías de la Información para la que la agilidad y la flexibilidad son indispensables; sin ese enfoque, tanto los costes como los propios servicios se ven afectados negativamente.

MORALEJA

Cuando los usuarios se preguntan por qué se ha llegado a esta situación la respuesta inmediata se orienta a las restricciones presupuestarias de los últimos años que han impedido el ritmo deseado de renovación de equipos. Ciertamente, el recurso económico juega un papel fundamental en el universo de las Tecnologías de la Información de cualquier organización, pero, como señala COBIT 5, en dicho ámbito la resolución de cualquier necesidad o problema exige actuar sobre varias palancas o catalizadores (drivers): principios, políticas y marcos de referencia; procesos; estructuras organizativas; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; personas, habilidades y competencias.

En línea con esa realidad, cabe subrayar la necesidad de seguir mejorando la madurez del Sistema de Gestión del Servicio, revisando el marco de roles y responsabilidades de cada uno de los procesos, a lo largo de todo el ciclo de vida de los servicios y, también, de los activos, desde su adquisición hasta su salida del entorno de operación, y discriminando, especialmente, quienes ejercen el rol de Proveedores de Servicio y quienes el de Clientes de dichos servicios.

Otros interrogantes habituales son los relacionados con los costes que para la organización supone la renovación de estaciones de trabajo o, también, el número de terminales de usuario que se precisan: En las propias cuestiones aflora cierta visión de las Tecnologías como una mera "commodity[10]" cuyo valor y relevancia para las tareas funcionales de negocio de los usuarios que consumen sus servicios

[9] **RACI** (ITIL 2011); un modelo usado como ayuda para definir una matriz de roles y responsabilidades. RACI significa Responsable de ejecutar (Responsible), Alto Responsable (Accountable), Consultados (Consulted), Informados (Informed). En cualquier proceso o servicio debe existir un único Accountable.

[10] **Commodity**: Mercancía, cualquier producto destinado a uso comercial. Al hablar de commodity, generalmente se hace énfasis en productos genéricos. Cuando determinada industria evoluciona, de modo que muchos participantes puedan realizar algo que antes solo podía realizar una determinada firma, se habla de "comoditización" de un producto o industria.

o utilizan sus activos suscita dudas. En ellas, más allá del elemental y condicionante estudio de las capacidades económicas de la organización para determinar el número de estaciones de trabajo que se pueden adquirir y gestionar, subyace el tradicional problema de alineamiento, y deseable integración, entre los procesos de negocio de la organización y sus recursos y capacidades de Tecnologías de la Información. Como acertadamente señalaba Antonio Sanz, responsable de Sistemas y Seguridad el Instituto de Investigación en Ingeniería de Aragón, el objeto de un proyecto de este tipo no era sustituir Windows XP por otro sistema operativo, sino apoyar los procesos de negocio. Las organizaciones buscan aumentar la productividad de sus empleados y aumentar la agilidad de sus servicios de negocio: responder a esas necesidades y capacitar al usuario para ello, de una forma eficiente, constituye el fundamento para utilizar tecnología.

Sin ningún género de dudas, la actualización del sistema operativo de las estaciones de trabajo de una organización pública no es un problema específico del personal técnico ni de la correspondiente Subdirección General: es una responsabilidad del órgano de gobernanza y dirección de las Tecnologías de la Información del departamento ministerial que implica una serie de distintos recursos, con su correspondiente ciclo de vida, a lo largo del tiempo; los técnicos deben limitarse a una gestión eficaz y, generalmente, eficiente de los activos de Tecnologías de la Información y, adicionalmente, a proporcionar al órgano de gobernanza corporativa los registros, métricas e indicadores necesarios para la toma de decisiones. Tanto los servicios como los activos de Tecnologías de la Información tienen unos costes que deben ser conocidos no solo por el Proveedor del Servicio y por el órgano de gobernanza corporativa, sino también por los clientes y usuarios consumidores; si dichos costes no encuentran su contrapartida en forma de aportación de valor a la operativa, tareas y resultados esperados de los Clientes, tal vez deba reconsiderarse su razón de ser.

Cualquier decisión estratégica sobre la selección de dicho sistema operativo estará basada en rigurosos y detallados casos de negocio que, naturalmente, tomarán en consideración todos los recursos y capacidades relacionados de Tecnologías de la Información a medio y largo plazo (personas, conocimiento, recursos económicos, capacidades de gestión, etc.): ello permitirá la elección entre un sistema operativo comercial interoperable con todas las aplicaciones comerciales del mercado o, en otro caso, un sistema operativo de software libre que, indudablemente, no resultará gratuito y precisará de unas fuertes capacidades y recursos para alcanzar la interoperabilidad con los centenares de aplicaciones comerciales y propietarias del Departamento. Tomada una decisión, el coste de la Gestión del Activo Sistema Operativo se incorporará a los procesos presupuestarios y de costes del Proveedor de Servicio de Tecnologías de la Información. En el caso particular del Ministerio de Defensa, debe tenerse en cuenta la magna complejidad que presenta la elección, transición a producción y operación diaria de un sistema operativo que debe convivir con cerca de quinientas aplicaciones y sistemas, de variada complejidad y, no pocas de ellas, soluciones propietarias. En Tecnologías de la Información las soluciones complejas, tanto desde el punto de vista de los propios productos como desde la perspectiva de sus procesos de gestión, resultan, generalmente, sinónimo de ineficiencias y de pérdida de eficacia.

Aspecto relevante de cualquier cambio de este impacto es la necesidad de una adecuada comunicación del mismo a la población de clientes y usuarios que se verán afectados. En este sentido, las comunicaciones y facilidades de autoayuda deben fundamentarse sobre el

correspondiente proceso de Gestión del Conocimiento que, inexorablemente, debe estar soportado en la herramienta de gestión del servicio, ITSM en su acrónimo inglés o SCANS en el ámbito del Ministerio de Defensa, y ser complementadas por las comunicaciones a través de la estructura orgánica.

En todo caso, las recomendaciones de los miembros de toda la comunidad de Seguridad de la Información no dejan resquicio alguno para las dudas:

- Centro Criptológico Nacional: *"La elaboración de un plan de migración del parque de equipos con sistema operativo Windows XP a versiones más actualizadas a la mayor brevedad posible".*
- Chema Alonso, de Eleven Paths: *"Tener un Windows XP en una administración pública (después del 8 de abril) sería una negligencia de tal envergadura merecedora, incluso, de denuncias por parte de los ciudadanos. Hacen falta recursos económicos; hay que migrar las aplicaciones por encima, cambiar los procesos, las herramientas de soporte y administración, las habilidades de los técnicos y los usuarios"*.
- David García y Antonio Ropero, de Hispasec: *"A los usuarios que aún siguen con XP, pocas opciones les quedan, migrar a otros sistemas como Android o Linux, actualizar a una versión superior de Windows, cambiar de ordenador… o quedarse expuestos a todo tipo de ataques, malware y problemas"*.

Conocidas las condiciones generadas por el escenario económico en los últimos años, más que nunca parece oportuno recordar la importancia crítica de los procesos de gestión: Como reza el quinto principio de la Calidad Total de Deming "***Mejorar constantemente el sistema de producción y servicios****: El sistema de producción, los servicios y la planificación deben contar con un proceso de mejora continua que nos permita mejorarlos constantemente y hacerlos más eficientes; pero ese proceso no será puntual, sino que deberemos realizarlo siempre: mejorar, mejorar y mejorar. Este sistema nos permitirá mejorar la calidad y la productividad, así como bajar los costes"*.

[i]

*Jesús Gómez Ruedas**
Teniente Coronel del Ejército de Tierra
Subdirección General de Tecnologías de la Información y Comunicaciones
Ministerio de Defensa

BIBLIOGRAFÍA

AENOR. UNE-ISO/IEC 19770-1 Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos, 2006

AENOR. UNE-ISO/IEC 20000-1 Tecnología de la Información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio, 2011

Cabinet Office. ITIL 2011, Information Technology Infrastructure Library, Reino Unido, 2011.

Centro Criptológico Nacional. Informe de Amenazas CCN-CERT IA-02/14. Riesgos de uso de Windows XP tras el fin de soporte, 2014.

Chema Alonso. http://www.elladodelmal.com/

Espiral Microsistemas. http://www.proactivanet.com

Hispasec Sistemas, SL. http://www.hispasec.com

ISACA. COBIT 5, Un marco de Negocio para el Gobierno y la Gestión de la Empresa, 2012.

itSMF España. http://www.itsmf.es

Kaspersky Lab. http://blog.kaspersky.es/

Microsoft Corporation. http://windows.microsoft.com/es-es/windows/lifecycle

Ozona Consulting, SL. http://www.ozona.es

Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

S2 Grupo. http://www.securityartwork.es

SecurityByDefault. http://www.securitybydefault.com/