

12/2011

8 noviembre de 2011

Jesús Gómez Ruedas

DIEZ AÑOS DEL PLAN DIRECTOR DE SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DEL MINISTERIO DE DEFENSA: CUADERNO DE BITÁCORA Y NUEVAS DERROTAS.

DIEZ AÑOS DEL PLAN DIRECTOR DE SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DEL MINISTERIO DE DEFENSA: CUADERNO DE BITÁCORA Y NUEVAS DERROTAS.

Resumen:

A principios del año 2002 el Ministerio de Defensa de España publicó su Plan Director de Sistemas de Información y Telecomunicaciones, iniciativa pionera en la Administración Pública española que pretendía modernizar las Fuerzas Armadas y alcanzar mayores niveles de eficiencia y calidad. Este documento examina las actividades desarrolladas a la luz de dicho Plan, profundiza en la vigencia del modelo de gestión de las Tecnologías de la Información que inspiró dicho Plan respecto a otros modelos y marcos de trabajo en boga y repasa el impacto que para dichas actividades ha supuesto el cuerpo normativo derivado de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos. Finalmente, antes de hacer balance y esbozar alternativas que puedan relanzar el papel de las Tecnologías de la Información de este Ministerio, integrándolas en las actividades de negocio consustanciales al mismo, repasa también los avances desencadenados por el Plan en materia de Seguridad de la Información y su interrelación con la Estrategia Española de Seguridad.

Abstract:

In early 2002, the Spanish Ministry of Defense published its Master Plan for Communication and Information Systems; it was a pioneering initiative in the Spanish Government oriented to modernize the Armed Forces and achieve higher levels of efficiency and quality. This paper examines the activities undertaken in the light of the Master Plan, builds on the validity of the Information Technology management model promoted by the Plan, in comparison with others current models and frameworks in fashion, and reviews the impact that legislation

Jesús Gómez Ruedas

resulting from the Law 11/2007, on electronic access of citizens to Public Services, has led to these activities. Finally, prior to balance and outline alternatives that may relaunch the role of Information Technology of the Ministry, integrating them into the business activities inherent to it, this paper also reviews improvements triggered by the Master Plan on Information Security and its interface with the Spanish Security Strategy.

Palabras clave:

Sistemas de Información y Telecomunicaciones, Tecnologías de la Información, Sociedad de la Información, Plan Director, eficiencia, gestión de servicios, gobierno corporativo, procesos, integración en el negocio, proveedor, cliente, usuario, buenas prácticas, generación de valor, activos, recursos, capacidades, ciclo de vida, administración electrónica, Seguridad de la Información, Estrategia Española de Seguridad, gestión de riesgos.

Keywords:

Communication and Information Systems, Information Technology, Information Society, Master Plan, efficiency, service management, corporate governance, processes, business integration, supplier, customer, user, best practices, value, assets, resources, capabilities, life cycle, e-government, Information Security, Spanish Security Strategy, risk management

Jesús Gómez Ruedas

Hace una década el mundo aún no había dejado de estremecerse tras los terribles atentados terroristas acaecidos en los Estados Unidos de América el 11 de septiembre de 2001; como consecuencia inmediata, se desencadenaban operaciones militares en Afganistán. Algunas semanas después, el 1 de enero de 2002, entraba en circulación en doce países europeos una nueva moneda única, el euro. Mientras tanto, en otro orden de cosas, Harry Potter había saltado de los libros a la gran pantalla, iniciando así una exitosa saga cinematográfica.

Entretanto, en el ámbito de las Tecnologías de la Información, las páginas web cumplían ya diez años desde que el físico Paul Kunz creara el primer sitio web de los Estados Unidos en los laboratorios del SLAC (Stanford Linear Accelerator Center); 1.600 millones de páginas HTML¹, 36 millones de servidores y 500 millones de internautas atestiguaban esta nueva “revolución industrial”; pero, además, se iniciaba la migración del protocolo IP (Internet Protocol) de su versión 4 a la 6, como consecuencia del previsible agotamiento del espacio de direccionamiento ante el exponencial aumento de la demanda. En España, el 17% de las empresas españolas ya operaba en este nuevo mundo virtual, frente a un promedio de un 20% de las empresas europeas o el 26% de las empresas norteamericanas.

Plan Director de Sistemas de Información y Telecomunicaciones²: Buscando vientos de modernidad y eficiencia

¹ HTML: Hyper Text Markup Language (Lenguaje de marcado de hipertexto)

² Sistemas de Información y Telecomunicaciones, ¿CIS, SIT, TIC o TI?:

A pesar de tratarse de un acrónimo en lengua inglesa, el uso del término CIS (Communication and Information Systems) está ampliamente extendido en el ámbito del Ministerio de Defensa; a diferencia de cualquier otro campo de actividad, en los que mayoritariamente se emplean acrónimos en lengua castellana distintos a los del entorno OTAN, ello alcanza incluso a las normas internas de alto rango del departamento. No obstante, el acrónimo SIT (Sistemas de Información y Telecomunicaciones) también es de uso generalizado, especialmente en el campo de la normativa de Seguridad de la Información. Sin embargo, una de las conclusiones de este trabajo será la constatación de lo trasnochado del enfoque del Sistema de Información y Telecomunicaciones como epicentro de la gestión de las tecnologías de información y comunicaciones. Ante esta realidad se ha acudido a las definiciones de una de las más recientes normas en este ámbito del principal foro y referente mundial, la Organización Internacional de Normalización (International Organization for Standardization, ISO); “ISO/IEC 38500:2008, Corporate Governance of Information Technology” define:

Tecnologías de la Información (TI): Recursos necesarios para adquirir, procesar, almacenar y difundir información. Este término también incluye las Tecnologías de la Comunicación (TC) y el término compuesto Tecnologías de Información y Comunicación (TIC).

Dado que el rol y la misión de las TI no distingue ámbitos de negocio (ya sea, por ejemplo, gestión de logística militar o gestión de personal de una empresa) ni tampoco cambia por su contenedor material (sea un ordenador personal, un cajero automático o un componente embarcado en un vehículo militar), este término será el utilizado en este documento.

Jesús Gómez Ruedas

Éste era el caldo de cultivo en el que se promulgaba, aquel mes de febrero del año 2002, la **Orden DEF/315/2002, por la que se aprobaba el Plan Director de Sistemas de Información y Telecomunicaciones** y se establecía, para su dirección, gestión y seguimiento, el Comisionado del Plan. Este Plan Director se enmarcaba en el Plan de Acción gubernamental INFO XXI, para el periodo 2001-2003, de la Administración General del Estado, en el ámbito de la Sociedad de la Información y las nuevas Tecnologías. Apelando a principios y criterios como la visión integral en relación a los ámbitos de negocio ministeriales, la organización y eficiencia de los recursos asignados o la calidad como un atributo de todas sus actuaciones,



el Plan se pergeñaba con la finalidad de establecer la política del Ministerio de Defensa respecto de las Tecnologías de la Información y Comunicaciones (TIC), determinando las necesidades y definiendo y priorizando las acciones precisas para el cumplimiento de dicha política.

Dicha Orden Ministerial encontraba sus orígenes en la **Directiva 134/1999 del Ministro de Defensa, sobre actuaciones para la elaboración de un Plan Director de Sistemas de Información**. En la misma se subrayaba el impacto de las nuevas tecnologías en las organizaciones de defensa y en los Ejércitos; al mismo tiempo, ligaba los procesos de modernización de las Fuerzas Armadas al empleo de las TIC, como imprescindibles instrumentos para multiplicar sus capacidades operativas. Como factores que explicaban la necesidad de dicho Plan emergían, entre otros, los siguientes:

- La conveniencia de normalizar sistemas, aplicaciones y metodologías,
- la consecución de un aprovechamiento óptimo de las infraestructuras, con una gestión más equilibrada de los recursos que permitiera una considerable reducción de los costes de adquisición y mantenimiento, o
- la mejora de la preparación técnica del personal, para alcanzar un mayor aprovechamiento y rendimiento de los recursos humanos, recursos con un alto grado de especialización y de los que se requeriría reducidos cortos periodos de adaptación en situaciones de movilidad.

Unos meses después, en noviembre del año 2000, la **Directiva 336/2000 del Ministro de Defensa** había colocado nuevos ladrillos en el futuro edificio de las TIC del Departamento, estableciendo las directrices que permitieran conseguir sinergias entre los órganos

Jesús Gómez Ruedas

competentes en los campos de la informática y las telecomunicaciones y que potenciaran la planificación, el control y la coordinación en este ámbito. Para ello, se determinó la creación en los Cuarteles Generales del Estado Mayor de la Defensa y de los tres Ejércitos de una “Célula de Planeamiento y Control CIS”, así como de una “Célula de Coordinación de la Gestión CIS”, durante el periodo de tiempo necesario para la elaboración y aprobación del Plan Director.

Las siguientes pinceladas permiten bosquejar el paisaje de estas tecnologías en el conjunto del Ministerio cuando despertaba el nuevo siglo:

- 924 emplazamientos con necesidad de emplear sistemas de información y telecomunicaciones en su actividad ordinaria.
- Al menos, unas 450 aplicaciones informáticas, en un entorno de ausencia casi total de sistemas corporativos y de falta de interoperabilidad entre los Sistemas de Información de los Ejércitos. De este escenario había resultado la existencia de un importante número de aplicaciones y sistemas duplicados, la ausencia de una metodología unificada para el desarrollo y adquisición de sistemas y, consecuentemente, una multitud de organismos con responsabilidad técnica en el desarrollo y mantenimiento de software.
- Carencia de flujos de información dentro de los sistemas y aplicaciones que se asociaran a los procesos de trabajo de las unidades de negocio.
- Unas 275 Redes de Área Local que desplegaban un parque estimado de unos 24.000 ordenadores personales.
- Una estructura costosa y voluminosa de grandes ordenadores implantados en diferentes centros de proceso de datos (Órgano Central³, Ejército de Tierra, Armada, Ejército del Aire, ISFAS⁴, INVIFAS⁵,...).
- Más de 20 plataformas y redes, distintas y no integradas, en el entorno de los Sistemas de Información de operaciones militares.
- 900 contratos distintos de servicios de telecomunicaciones con la misma operadora.
- Más allá de los tradicionales entornos militares de manejo de información clasificada, habitualmente en soporte papel, ausencia de un cuerpo normativo homogéneo y de estructuras de seguridad corporativas que permitieran conjugar la protección de la información con su uso compartido cuando fuese necesario.
- Una desagregación de los recursos económicos destinados a Tecnologías de la Información (repartidos en programas de adquisición, de investigación y

³ Denominación oficiosa empleada para identificar el entorno de los órganos administrativos ubicados, fundamentalmente, en la sede central del Ministerio del paseo de la Castellana de Madrid.

⁴ ISFAS: Instituto Social de las Fuerzas Armadas

⁵ INVIFAS: Instituto para la Vivienda de las Fuerzas Armadas

Jesús Gómez Ruedas

desarrollo,...), que eran gestionados por más de una veintena de organismos gestores.

- Un amplio y variado espectro de recursos humanos con algún tipo de formación en esta área de conocimiento (oficiales especialistas en informática, oficiales especialistas en comunicaciones, oficiales ingenieros de los tres ejércitos, suboficiales pertenecientes a cuerpos militares de informática y comunicaciones, personal civil propio, personal civil contratado, ...), que venían siendo gestionados por diferentes órganos gestores de Recursos Humanos, desde la perspectiva parcial de cada uno de ellos. La situación se veía agravada por una percepción de falta de motivación en el seno de algunos de dichos colectivos.
- Unas estructuras orgánicas dispersas y distribuidas en los diferentes ejércitos, sede central del Ministerio y Organismos Autónomos, en las cuales se realizaban las mismas actividades, con alcance limitado a sus correspondientes ámbitos, y con unas líneas de coordinación tenues, cuando no inexistentes.

Para responder a este complejo y singular escenario en el que venían a converger ámbitos de negocio tan dispares como, entre otros, la sanidad, la enseñanza, la gestión de infraestructuras, la conducción de operaciones militares, la gestión de personal, la gestión de logística, la justicia, la gestión del medio ambiente o la acción social, el 22 de febrero de 2002 el Boletín Oficial del Ministerio de Defensa

alumbraba la citada Orden DEF/315/2002. La política definida por este ambicioso Plan Director contemplaba, de forma integral, todos los aspectos relacionados con estas tecnologías, recogiendo los principios básicos de cualquier organización moderna e incluyendo las características específicas del Ministerio de Defensa. Éstas eran las líneas generales enunciadas por dicha política:



- Identificación a lo largo y ancho del Departamento, incluidos Organismos Autónomos, de 8 áreas funcionales, cuyos procesos de negocio se articulaban sobre una serie de Sistemas de Información explicitados para cada una de ellas.
- Impulso al software comercial en detrimento de los desarrollos propios.
- Una plataforma informática definida por: dos Redes de Área Extensa completamente segregadas (Propósito General y Mando y Control Militar); la concentración de los diversos centros de proceso de datos existentes en uno único ubicado en dos emplazamientos distintos; un modelo de datos único e integrado; una única

Jesús Gómez Ruedas

plataforma tecnológica de interoperabilidad básica (mensajería, trabajo en grupo,...) con un dominio en cada WAN⁶; un servicio de directorio basado en un modelo de dos directorios (uno por WAN) sobre la base de un mismo producto; una Infraestructura de Clave Pública (PKI⁷), con una única Entidad de Certificación raíz y una Entidad de Certificación delegada para cada WAN; la implantación de tarjetas electrónicas como soporte de los certificados; la definición de una Arquitectura Técnica y de Aplicaciones única para todo el Ministerio.

- Una plataforma de telecomunicaciones articulada sobre: una única Red Global de Telecomunicaciones compuesta por dos dominios integrados e interoperables, uno integrado en el Sistema de Telecomunicaciones Militares y otro constituido por una Red Privada Virtual (RPV) para voz y otra red para datos, ambas sobre recursos externos; la contratación centralizada de ambas redes externalizadas.
- La elaboración de un Plan de Seguridad del Ministerio y la creación de la estructura que lo gestionara.
- Desde la perspectiva de la gestión de recursos económicos, la concentración en un único subprograma de todos los créditos relativos a Sistemas de Información y Comunicaciones, así como la reducción del número de centros de coste que venían gestionándolos.
- Unas directrices relativas a los Recursos Humanos consistentes en: la determinación de las necesidades reales globales de personal técnico y la definición de su perfil; el impulso de un modelo de carrera y la creación de un plan de motivación que hiciera atractivo el desarrollo profesional en este campo; el empleo de recursos externos dentro del modelo de gestión de las Tecnologías de la Información.
- La necesidad de una estructura orgánica con capacidad de llevar a cabo la Política establecida por esta Orden Ministerial.

Para abordar este ingente desafío se establecían:

- Un plazo de tiempo de cuatro años, hasta enero de 2006.
- 50 objetivos, desglosados en 242 acciones, que se articulaban mediante un Plan de Gestión, un Plan de Arquitectura y Plataforma Tecnológica y, por último, un Plan de Obtención y Modernización de los Sistemas de Información.

⁶ WAN: Wide Area Network (Red de Área Extensa)

⁷ PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

Jesús Gómez Ruedas

En definitiva, un plan innovador que, en su época, constituyó un referente para toda la Administración Pública española. De sus líneas básicas se puede inferir una apreciable focalización en las plataformas y soluciones tecnológicas, una fuerte orientación hacia los propios Sistemas de Información y, finalmente, un loable deseo de identificar los procesos de negocio de todo el Ministerio por medio de su asociación a dichos sistemas.



En octubre de 2005, en el marco del Plan de Modernización de la Administración Militar 2005-2008, el Secretario de Estado de Defensa aprobó el documento “Objetivos estratégicos a corto plazo en el marco del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa”, que, en la práctica, suponía una revisión del citado

plan. El documento establecía los siguientes objetivos estratégicos:

1. Implantación del Sistema de Mensajería Oficial del Ministerio de Defensa (SIMENDEF).
2. Implantación de la Infraestructura de Seguridad (Infraestructura de Clave Pública, Tarjeta Electrónica del Ministerio de Defensa y desarrollo normativo).
3. Colaboración proactiva con el Plan Estratégico de la Oficina de Modernización de la Administración Militar (OMAM).
4. Implantación del Sistema de Información de Sanidad del Ministerio de Defensa en un centro hospitalario.
5. Implantación del Sistema Global de Gestión del Conocimiento del Ministerio de Defensa (Intranet corporativa, Campus Virtual y puesta en funcionamiento de comunidades de prácticas y grupos de trabajo virtuales).
6. Pilotaje y validación de la plataforma tecnológica que deberá dar soporte a la Gestión Económica del Ministerio de Defensa.
7. Dotar a la Dirección General de Personal de un Sistema de Simulación y Análisis de datos de Recursos Humanos.
8. Implantación del Sistema de Gestión de Infraestructura del Ministerio de Defensa.
9. Implantación de Windows 2000 en el Ministerio de Defensa.
10. Plan de Continuidad. Centro de Respaldo.
11. Renovación Tecnológica de ordenadores personales y servidores.

Jesús Gómez Ruedas

Pero, antes de continuar con el devenir de las actuaciones que se iniciaron con aquel Plan, tal vez sea momento de hacer un alto, recuperar el aliento y echar la vista sobre la evolución y el rol de estas tecnologías en el marco de las organizaciones modernas.

Una ciencia bisoña

Mucho ha llovido desde aquellos años 70 en los que no existía la figura del Director de Informática (CIO⁸) ni, tan siquiera, abundaban departamentos formales de informática. Surgían las primeras aplicaciones comerciales y los técnicos de las corporaciones trabajaban en estrecho contacto con aquel otro personal que conocía y conducía el negocio; las metodologías no se habían normalizado aún y, sin solución de continuidad, se diseñaban nuevas formas de operación, al mismo tiempo que los sistemas de información se adaptaban y amoldaban a esas operativas actualizadas; la interacción y la comunidad de ideas entre la gente del negocio y su soporte de tecnologías constituía una práctica común; como consecuencia inmediata, los escalones directivos de las organizaciones percibían y valoraban el impacto que para su negocio suponía una inversión suficiente y un empleo adecuado de las Tecnologías de la Información.

Los años 80 conocieron espectaculares avances en materia de prestaciones de las plataformas de hardware. Más tarde, en la década de los 90, serían los componentes software los que protagonizaran el trepidante progreso del “planeta informático”, originando, de paso, un descenso en los astronómicos precios del equipamiento hardware. Con la entrada del nuevo siglo, un nuevo “personaje”, de nombre Internet, vino a revolucionar este universo. Mientras tanto, aunque las capacidades de hardware y el software se habían multiplicado de forma extraordinaria, el esplendor y las luces de los primeros tiempos se habían visto atenuados por las primeras sombras entorno al empleo de estas herramientas: Con frecuencia, los proyectos no llegaban a término de forma exitosa o los costes iniciales se disparaban de forma escandalosa; la operativa de las organizaciones se veía paralizada ante el desempeño poco fiable de algunos sistemas de información, lo que, a su vez, producía pérdidas de tiempo y de productividad de los usuarios e, incluso, daños a la imagen corporativa; las inversiones en TI de las organizaciones se disparaban hasta el extremo de hacer dudar a sus máximos dirigentes de la rentabilidad de las mismas; en resumen, con no poca frecuencia, los departamentos de TI eran percibidos más como una carga que como una ayuda para el negocio. Definitivamente, dichos departamentos tenían



⁸ CIO: Chief Information Officer

Jesús Gómez Ruedas

que abandonar aquella existencia discreta y casi anónima para el resto de la organización; ya no era posible continuar siendo ese nicho de las organizaciones que, con niveles de madurez que algún modelo público de referencia describiría posteriormente como “Apagar incendios”, se dedicaba básicamente a construir aplicaciones, montar la infraestructura tecnológica para que éstas funcionaran y explotaras o hacerlas funcionar.

También hacia el año 2000 se había publicado la versión 2 del marco de buenas prácticas ITIL⁹, creado años atrás en el seno de la Administración Pública británica. Se trataba del compendio de mejores prácticas de gestión de Tecnologías de la Información más ampliamente extendido e implantado en la industria. El objetivo de ITIL se puede resumir en alinear la Tecnología en el Negocio por medio de una gestión de servicios de TI basada en procesos.

ITIL sería uno de los principales pilares sobre los que, cinco años más tarde, se levantara la norma ISO/IEC 20000:2005 “Tecnología de la Información. Gestión del Servicio”; aparece, por tanto, un nuevo enfoque: **la gestión de servicios de Tecnologías de la Información**. La “Gestión de Servicios de TI” no es otra cosa que un conjunto de capacidades organizativas especializadas cuyo fin es generar valor para los clientes (ya sean externos o internos) en forma de servicios. El objetivo de la norma es proveer un sistema de gestión que incluya las políticas y el marco de trabajo para hacer posible una efectiva gestión e implementación de todos los servicios de TI. Este año 2011 ha sido testigo de la publicación de una nueva versión de la norma, la ISO/IEC 20000:2011.



Pero en la búsqueda de la eficiencia en el empleo de las Tecnologías se seguían detectando lagunas: Muchas organizaciones venían utilizando las TI como una herramienta fundamental para su negocio y, probablemente, pocas podrían funcionar eficazmente sin ellas; pero, además, las TI se habían constituido en un factor importante en los futuros planes de negocio de muchas organizaciones. En cambio, con cierta frecuencia, no se obtenía el rendimiento esperado de las cuantiosas inversiones relacionadas con las TI: si existía un problema, éste se informatizaba... ¡pero no se resolvía! La principal razón de esos resultados negativos no era otra que haber concedido mayor importancia a la propia tecnología, los aspectos financieros o los de planificación de las actividades de TI, que al contexto global del uso de las TI en el negocio. Aparece entonces una nueva habilidad y competencia directiva que viene a satisfacer esta necesidad de control y, en definitiva, este ejercicio de responsabilidad corporativa: **el gobierno corporativo de las**

⁹ ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructuras de Tecnologías de la Información)

Tecnologías de la Información. Es en el año 2008 cuando se publica la norma **ISO/IEC 38500:2008 “Corporate Governance of Information Technology”**, donde se define que *“el Gobierno Corporativo de las TI es el sistema mediante el cual es dirigido y controlado el uso presente y futuro de las Tecnologías de la Información y las Comunicaciones dentro de la Organización”*. Especifica la norma que es una parte integrante del Buen Gobierno Corporativo y, como tal, una responsabilidad del Consejo de Administración, u órgano equivalente, y del equipo de Alta Dirección de la organización (independientemente de la presencia o ausencia en el mismo del departamento de informática).

Pero mientras todas estas capacidades se van asentando en la cultura de las organizaciones y las responsabilidades asociadas quedan nítidamente definidas, los viejos usos y costumbres continúan seriamente enraizados en muchas corporaciones. En el fondo, no son sino indicadores de ese distanciamiento y esa falta de integración entre los procesos de negocio y los modelos de gestión de los departamentos técnicos: aquí, clientes internos de negocio que no expresan sus necesidades de implantación de tecnología por medio de requisitos operativos, sino que pretenden imponer una determinada solución de mercado desde el desconocimiento de los elementos que articulan las capacidades del prestador interno de tecnología (personas, procesos, recursos tecnológicos y entidades colaboradoras); allá, un proveedor interno de servicios de tecnología que interpreta las necesidades operativas de sus clientes y realiza, de forma autónoma, adquisiciones en base a su entendimiento de cómo debe funcionar el negocio; acullá, un sinfín de unidades de negocio que pugnan por un presupuesto común y limitado desde el desconocimiento de las prioridades establecidas por el Consejo de Administración u órgano equivalente.



La historia de las Tecnologías de la Información es breve y esa juventud es, frecuentemente, sinónimo de errores o de precipitaciones y, casi siempre, de falta de madurez. Del mismo modo que ningún comprador inmobiliario le indicaría a un arquitecto cómo debe diseñar la casa que piensa adquirir o que ningún paciente le señalaría al doctor la prescripción que debe recetarle frente a sus propias dolencias, parece evidente que muchas organizaciones precisan todavía algunos giros más de su “torno de alfarero” hasta conseguir tornear el modelo de servicios de Tecnologías de la Información que mejor se adapte a sus necesidades operativas y a sus capacidades económicas, consiguiendo así la mejor integración posible entre procesos de negocio y TI.

Aunque el espectro de normas relacionadas con un empleo oportuno, eficaz y eficiente de las Tecnologías de la Información no se detiene, ni mucho menos, aquí (baste recordar ISO

Jesús Gómez Ruedas

9001, de gestión de Calidad; ISO 14001, de gestión medioambiental; ISO 15504, de evaluación de procesos de desarrollo de software; ISO 27001, de seguridad de la información; UNE¹⁰ 71599, de gestión de la continuidad del negocio; ISO 27031, de disponibilidad de las TI para la continuidad del negocio; ISO 19770, de gestión de activos de software; sus correspondientes normas AQAP¹¹ adaptadas para el entorno OTAN, cuando las necesidades de manejo de información, así lo requieran;...), el objeto y extensión de este documento aconsejan centrarse en los profundos, innovadores y trascendentales conceptos de Gobierno Corporativo de TI y Gestión de Servicios de TI.

Gobierno de las Tecnologías de la Información

Este innovador concepto encuentra su origen en la definición de Gobierno Corporativo publicada como un Informe de la Comisión sobre los Aspectos Financieros del gobierno de las Sociedades Públicas (**el Informe Cadbury**¹²) en 1992. A su vez, el Informe Cadbury también aportó la definición básica de Gobierno Corporativo a los **Principios de Gobierno Corporativo de la OCDE**¹³ de 1999 (revisados en 2004). El buen gobierno implica la existencia de políticas, estrategias y controles orientados a la consecución de los objetivos y a garantizar que las corporaciones utilizan sus recursos de una manera eficaz, además de asegurar la existencia de un sistema para el control y gestión de los recursos.

El concepto de “Gobierno Corporativo de las Tecnologías de la Información” desarrollado por la ISO/IEC 38500:2008 integra e institucionaliza las buenas prácticas para garantizar que las TI en la organización soportan los objetivos

del negocio. De esta manera, el gobierno de TI **facilita que la corporación aproveche al máximo su información**, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Por lo tanto, para proporcionar la información que la institución requiere para lograr sus objetivos, **la empresa necesita invertir en, y administrar**



¹⁰ UNE: Una Norma Española

¹¹ AQAP: Allied Quality Assurance Publication (Publicación Aliada de Aseguramiento de la Calidad)

¹² Informe Cadbury: Informe elaborado por un Comité de entidades públicas del Reino Unido (Bolsa de Londres, asociación profesional de contables y otras) y publicado en diciembre de 1992 con el fin de estudiar aspectos financieros y de control de las sociedades. Constituye una referencia imprescindible en el ámbito de la auditoría.

¹³ OCDE: Organización para la Cooperación y el Desarrollo Económico.

y controlar, los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

Además de ayudar a las máximas autoridades de la entidad (propietarios, miembros del consejo, directivos, socios, altos ejecutivos o similares) a comprender y cumplir con sus obligaciones legales, reglamentarias y éticas respecto al uso que, en sus organizaciones, se hace de las TI, este sistema de controles y garantías proporciona un marco de principios para los Administradores de la organización cuando evalúen, dirijan y supervisen el uso de las tecnologías de la información (TI) en el seno de la misma:

- **Responsabilidad:** Los individuos y grupos dentro de la organización comprenden y aceptan sus responsabilidades respecto de la demanda y la prestación de servicios de TI. Quienes tienen la responsabilidad sobre acciones también tienen la autoridad para llevarlas a cabo.
- **Estrategia:** La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TI; los planes estratégicos de TI satisfacen las necesidades actuales y futuras de la estrategia de negocio.
- **Adquisición:** Las adquisiciones de TI se hacen por razones válidas, sobre la base de análisis adecuados y continuados, a través de decisiones claras y transparentes. Hay un adecuado equilibrio entre beneficios, oportunidades, costes y riesgos, tanto a corto como a largo plazo.
- **Rendimiento:** Las TI son adecuadas para el propósito de dar soporte a la organización, mediante la provisión de servicios, niveles de servicio y calidad de servicio requeridos para alcanzar las necesidades presentes y futuras del negocio.
- **Cumplimiento:** Las TI cumplen con toda la legislación y regulación obligatorias.
- **Conducta humana:** Las políticas, prácticas y decisiones relacionadas con las TI muestran respeto hacia la Conducta Humana, incluyendo las actuales y futuras necesidades de todos los “individuos implicados en el proceso”.



La norma proporciona líneas directrices para los Administradores de las organizaciones sobre el uso eficaz, eficiente y aceptable de las Tecnologías de la Información (TI) en sus organizaciones. Se aplica al gobierno de los procesos (y decisiones) de gestión relativos a los servicios de información y comunicación utilizados por una organización. Estos procesos podrían ser controlados tanto por

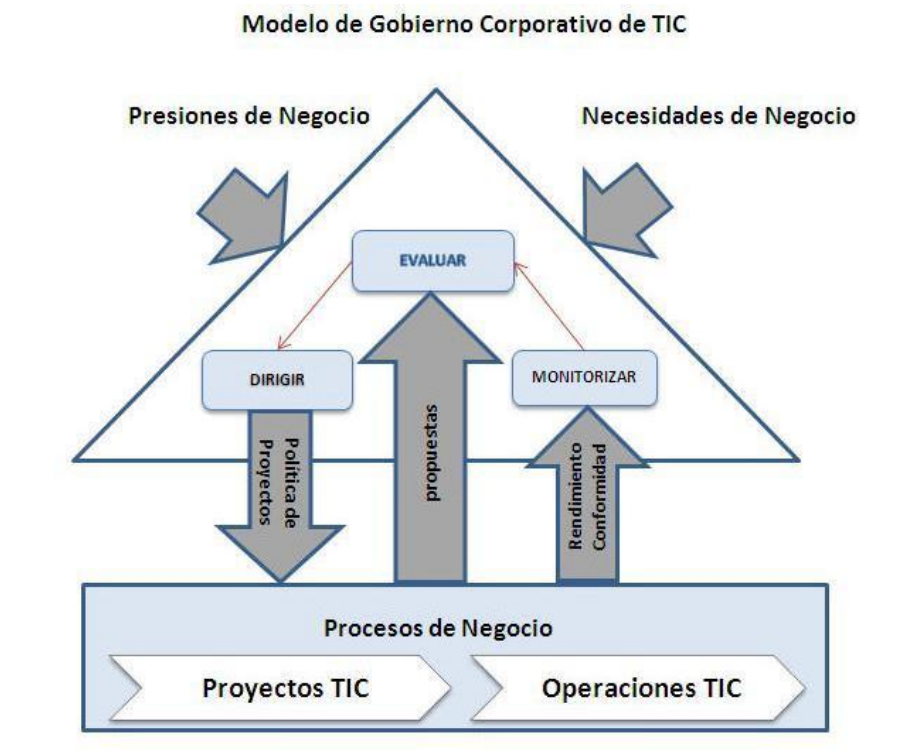
Jesús Gómez Ruedas

especialistas en TI de la organización como por proveedores de servicios externos, o unidades de negocio dentro de la organización.

El citado marco de buen gobierno de las TI se completa con un modelo que define las tres tareas principales que deben desarrollar los Administradores de la corporación:

- Evaluar el uso actual y futuro de las TI.
- Dirigir la preparación y ejecución de planes y políticas para asegurar que el uso de las TI satisface los objetivos empresariales.
- Monitorizar el cumplimiento de las políticas y el desempeño respecto de lo planificado.

Por lo tanto, en tiempos de ajustes económicos y de búsqueda permanente de soluciones imaginativas y eficientes, parece obligatorio no despreciar las herramientas y buenas prácticas que, importadas de otras comunidades profesionales y de otros ámbitos ajenos a las TI, han demostrado ser útiles para auxiliar a los Administradores de las organizaciones, ya sean públicas o privadas, a equilibrar los riesgos y fomentar oportunidades derivadas de la utilización de las Tecnologías de la Información.



Gestión de las Tecnologías de la Información

Las preocupaciones, los principios, las responsabilidades, los riesgos analizados y las decisiones que emanen del ámbito de la alta dirección de la organización, conforme a sus

Jesús Gómez Ruedas

habilidades y capacidades en materia de Gobierno Corporativo de las Tecnologías de la Información, constituirán la base de partida para que el Departamento de TI pueda ordenar y estructurar sus propios procesos, sus actividades y sus variados recursos en perfecta consonancia e integración con las necesidades operativas del negocio. Éste es el campo natural de la Gestión de las TI y éste es el espacio de actuación del personal técnico en sus diversos perfiles profesionales. Sin Gobierno de las TI, el éxito en la Gestión de las TI se torna una misión imposible: El gobierno corporativo y la gestión están claramente diferenciados, ya que el primero permite la generación de unas condiciones en las que los responsables de la gestión de TI pueden realizar sus tareas de forma eficaz.

Es bastante frecuente concebir el servicio TI en términos de tecnología, ignorando los procesos de negocio: Se habla de actualizar la base de datos, de adquirir un nuevo hardware o de desplegar un nuevo producto software, pero ninguna de estas afirmaciones describe la necesidad del negocio para realizar dichas tareas. **La estrategia de los actuales modelos de referencia** (como UNE-ISO/IEC 20000) **para integrar las Tecnologías de la Información en el Negocio se basa en la adopción de procesos en lugar de fundamentarse en la infraestructura tecnológica.** Esos procesos deben permitir el alineamiento continuo de las TI con las necesidades operativas de las unidades de negocio. En las modernas organizaciones las TI forman parte de un creciente número de bienes y servicios a los que da soporte. También en el mundo de los negocios ha cambiado el rol de la provisión de información: **las TI ya no sirven solo de soporte, sino que se han convertido en la base para la generación de valor empresarial.**

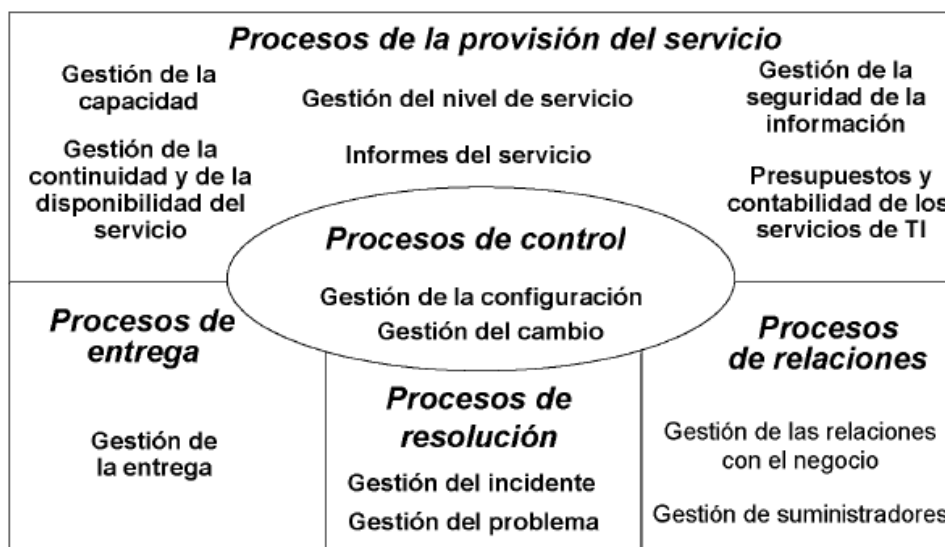
Dentro de la Gestión de las TI se enmarca la **Gestión de Servicios de TI**, pero, ¿qué es un servicio de TI? Pues un medio de **entregar valor a los clientes** facilitándoles los resultados que buscan obtener, sin asumir la propiedad de los costes ni los riesgos específicos. El paradigma del servicio de TI está generando un enorme cambio cultural dentro de las organizaciones, ya que deben adecuarse lo antes posible para beneficiarse de las ventajas derivadas de una buena gestión. De este modo, como ya se ha indicado, se establece una nueva relación entre los servicios de información y el negocio, convirtiéndose aquellos en proveedor interno que “vende” sus servicios TI y que, por tanto, debe garantizar la calidad de los mismos. Al mismo tiempo, la “venta” de servicios TI deriva en un fortalecimiento del control de costes que garantice la rentabilidad de las inversiones en infraestructuras. De la misma forma, el departamento de TI dependerá de otros departamentos internos y, normalmente, también de proveedores externos.



Jesús Gómez Ruedas

Se define la Gestión de Servicios TI como un **conjunto de capacidades especializadas de la organización** cuyo fin es **generar valor** para los **clientes** en forma de **servicios**. Dichas capacidades adoptan la forma de Funciones y Procesos. Sin dichas capacidades, una organización no sería otra cosa que una amalgama de recursos que, por sí mismos, tendrían poco valor. La Gestión de Servicios de TI es la disciplina y procedimientos para asegurar los niveles de servicio que se han comprometido. Para ello se precisa el concurso, en correcta armonía, de cuatro elementos:

- Las personas, que cumplen funciones en la organización y roles en los procesos.
- Los procesos, que organizan la gestión de los productos.
- Los productos tecnológicos, que representan los elementos de la infraestructura TI.
- Los colaboradores de la organización (por ejemplo, proveedores), que prestan apoyo dentro de los procesos y en la gestión de los productos.



Procesos de gestión del servicio según ISO 20000:2005

Cambio de paradigma: De los Sistemas de Información a los Servicios de Tecnologías de la Información

Si se analiza esa efímera historia del “reino de las comunicaciones y el tratamiento de la información” resulta sencillo percibir como el foco ha ido desplazándose, a lo largo de los años, de los actores principales, más clásicos, veteranos y, ciertamente, incuestionables, a otros figurantes menos conocidos, más etéreos, pero imprescindibles para poder obtener los beneficios y el impacto esperado de aquéllos: Al principio, los dispositivos físicos irrumpieron deslumbrantes en las postrimerías de la Sociedad Industrial, con precios desorbitantes que

Jesús Gómez Ruedas

los hacían accesibles solo para una minoría. Años después, se puso de manifiesto cómo las capacidades del software multiplicaban de forma casi infinita las potencialidades del hardware. Más tarde, las redes y, especialmente, internet permitieron intuir la omnipotencia del intercambio de información, de la ubicuidad de datos e informaciones o de la capacidad del procesamiento distribuido. Pero, simultáneamente, todo este universo de dispositivos físicos y lógicos se había vuelto tan amplio, tan diverso y tan complejo, en un periodo de tiempo realmente corto, que se había tornado, frecuentemente, ingobernable; de algún modo, podría aplicarse a la situación aquella máxima de “morir de éxito”.

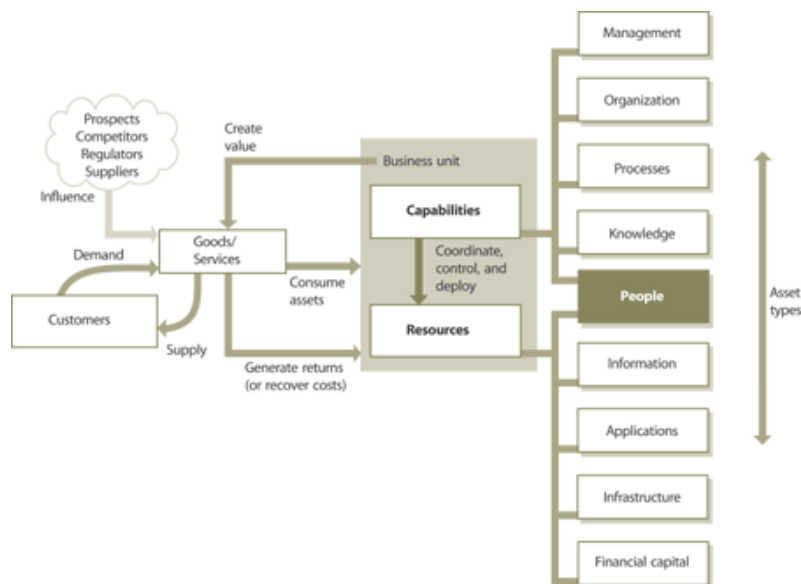


Ello llevó a organizaciones de todo el mundo, públicas y privadas, a investigar las razones por las que unas inversiones tan importantes no aportaban a las organizaciones el retorno esperado y cómo estas poderosas herramientas pudieran constituir un elemento de valor diferencial para dichas corporaciones. Es así como nacen metodologías, estándares y modelos de referencia relativos a la gestión de las TI y, posteriormente, directrices para el buen gobierno corporativo de las TI. Frecuentemente, todos esos modelos se basan en las denominadas “Buenas Prácticas”; no son otra cosa que “la forma aceptada de hacer que algo funcione”. Estas prácticas no garantizan el éxito, pero aumentan las probabilidades de alcanzarlo. Las Buenas Prácticas se basan en el conocimiento de expertos y en las experiencias exitosas de quienes lo han hecho y documentado con anterioridad. Según su tipo de actividad, los problemas y preocupaciones de muchas organizaciones son, en gran parte, similares: Si alguien se ha enfrentado con situaciones parecidas y ha documentado el modo de resolverlas, ¿por qué despreciar ese conocimiento?, ¿para qué tropezar en la misma piedra?, ¿por qué pretender reinventar la rueda? Se entra así en una nueva época orientada a identificar los modelos de gestión de las tecnologías de la información (cómo gestionar todas estas capacidades del modo más eficiente posible, reduciendo al máximo los riesgos) y los modelos de gobierno de las TI (cómo deben emplear las TI los dirigentes de las organizaciones para obtener el máximo beneficio en sus áreas de negocio). Es evidente que el éxito no viene de la mano de abundantes recursos, sino, por el contrario, de la buena gestión de los recursos y de un adecuado y responsable ejercicio de las tareas directivas.

En el presente, **las organizaciones precisan activos en lugar de recursos**. Se define “activo” como los recursos y capacidades utilizados por las organizaciones para crear valor en forma de bienes y servicios. Es la creación de valor lo que convierte a un elemento en un activo; un mismo elemento puede ser un activo para una organización y no serlo para otra, debido a la incapacidad de esta última para crear valor con él.

Jesús Gómez Ruedas

Las organizaciones proporcionan a los clientes los bienes y servicios que estos demandan. Al mismo tiempo, deben utilizar sus activos para producir esos bienes y servicios, creando valor en el proceso. El siguiente gráfico describe el papel de los activos en las organizaciones.



Las unidades de negocio son conjuntos de activos coordinados y orientados a objetivos

Los recursos son los elementos directos para la producción. **Son recursos el capital financiero, la infraestructura, las aplicaciones, la información y las personas.** Las capacidades se utilizan para transformar los recursos; **son capacidades la gestión, la organización, los procesos, el conocimiento y las personas.** Por tanto, las personas son, a la vez, recursos y capacidades. **Las capacidades representan la habilidad de las organizaciones para coordinar, controlar y desplegar los recursos con el objetivo de crear valor.** Esas capacidades se encuentran contenidas en las personas, los procesos y los sistemas de las organizaciones. Adquirir recursos es fácil, conseguir capacidades es mucho más complejo y éste es, precisamente, el objetivo.

Un último concepto imprescindible en este nuevo paradigma es el de **ciclo de vida**, es decir, la secuencia de estados por los que pasa el activo o el servicio desde su obtención hasta su retirada. Como puede observarse en el gráfico anterior, centrarse exclusivamente en el ciclo de vida de los cinco tipos de recursos sería absolutamente insuficiente para que los clientes, y sus usuarios, pudieran disponer de los servicios TI necesarios para potenciar la eficacia y la eficiencia de sus actividades operativas.

Administración Electrónica: Derechos, deberes y maremágnum

De regreso al ámbito nacional, en medio de este hervidero de normas, metodologías y buenas prácticas internacionales, siempre orientadas a la búsqueda de los mayores niveles

Jesús Gómez Ruedas

de eficiencia y de la diferenciación respecto a otras corporaciones similares por medio del buen empleo de las TI, la Administración Pública española también empezaba a dar sus primeros pasos.

En mayo de 2005, mientras el Ministerio de Defensa ya ejecutaba su Plan Director, veía la luz el **Real Decreto 589/2005, de reestructuración de los órganos colegiados responsables de la Administración Electrónica**. El objeto de esta norma no era otro que **establecer las líneas estratégicas**, dentro de la política del Gobierno, en materia de **tecnologías de la información**, así como impulsar y coordinar el desarrollo de la Administración electrónica en la Administración General del Estado y adoptar medidas para su ordenada implantación. Como consecuencia del mismo el **Consejo Superior de Informática** pasó a denominarse **Consejo Superior de Administración Electrónica**; al mismo tiempo, se creaban las Comisiones Ministeriales de Administración Electrónica que, sustituyendo a las anteriores Comisiones Ministeriales de Informática, se constituían en instrumentos para la coordinación interna de cada departamento en materia de tecnologías de la información y de Administración Electrónica. Al margen de directrices relacionadas con los procesos de contratación en materia de tecnologías de la información, la **principal novedad** era el mandato a cada ministerio para que **se elaborase un plan estratégico departamental** que recogiera de forma concreta los servicios que el ministerio tuviera previsto desarrollar, especialmente los dirigidos a ciudadanos y empresas, su planificación temporal, los recursos humanos y financieros necesarios y los contratos que se debieran realizar. Especificaba, además, que el concepto de plan estratégico debería interpretarse en sentido amplio, ya que



debía **abarcar todos los sistemas de información necesarios para responder a los objetivos estratégicos departamentales** y, por tanto, tendría que incluir a los denominados planes directores y planes de sistemas.


Por su concurrencia con las actividades que había articulado el Ministerio de Defensa desde el mes de febrero de 2002, conviene, en este punto, recapitular las consecuencias prácticas de este Real Decreto para dicho departamento:

- Un órgano colegiado interdepartamental que cambia su nombre de “Consejo Superior de Informática” por el de “Consejo Superior de Administración Electrónica”.
- El cambio de denominación de la “Comisión de Informática del Ministerio de Defensa”, creada por Orden 52/1987, por el de “Comisión Ministerial de Administración Electrónica del Ministerio de Defensa”.

Jesús Gómez Ruedas

- La necesidad de alinear el entonces vigente Plan Director de Sistemas de Información y Telecomunicaciones con el demandado Plan Estratégico, en el que ahora también se incluían los servicios destinados a ciudadanos y empresas, y que, naturalmente, debía incluir **todos los sistemas de información necesarios para responder a los objetivos estratégicos del departamento.**

Sin entrar a considerar los modelos o estructuras de gestión de las TI vigentes en el Ministerio de Defensa, se puede concluir que las implicaciones eran moderadas: el cambio de la etiqueta “Informática” por la de “Administración Electrónica” (como muestra de la preocupación del legislador por mejorar los servicios directos al ciudadano por medio de las TI) y la necesidad de revisar el vigente Plan Director de Sistemas de Información y Telecomunicaciones para promoverlo a la categoría de Plan Estratégico; plan que continuaría definiendo la política corporativa respecto a recursos humanos y financieros, su planificación y seguiría abarcando todos los sistemas de información necesarios para responder a los objetivos estratégicos departamentales.



Tus trámites y gestiones más fáciles y desde casa

Por fin, la dilatadamente esperada y deseada “ley de administración electrónica” hizo su presentación en

sociedad en junio de 2007, bajo el nombre de “Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos”. De su propio título se infiere una especial preocupación, ya mostrada por el Real Decreto 589/2005: subrayar que el foco de esta ley se encuentra sobre los ciudadanos en tanto que destinatarios de una buena parte de la actividad de las Administraciones Públicas. Ciertamente, esta perspectiva pudiera implicar cierto grado de desconcierto o desenfoque en Ministerios en los que, como es el caso del de Defensa, estos procesos de negocio orientados directamente al ciudadano son de carácter y alcance minoritario y, además, no se encuentran entre los que puedan permitir la medición de la eficacia o la eficiencia de los procesos de negocio fundamentales del departamento, ya que estos se relacionan directamente con la operatividad de las Fuerzas Armadas.

La ley se centra en reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medio de las tecnologías de la información, pero también dispone que aquéllas deberán utilizar las TI asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias (es decir, define objetivos de la gestión de TI). De hecho, entre las finalidades de la ley se encuentra la de *“contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la*

Jesús Gómez Ruedas

eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones". Tras la citada enunciación de derechos y deberes, la ley se sumerge directamente en conceptos y criterios donde se vinculan el régimen jurídico y los mecanismos tecnológicos que deben garantizarlo (sedes electrónicas, elementos de identificación y autenticación, registros, comunicaciones y notificaciones electrónicas, etc.). Por el contrario, no se consideró necesario la definición de principios o modelos que pudieran servir de guía a los responsables del buen gobierno corporativo de las TI (sistema de dirección y control del uso actual y futuro de las Tecnologías de la Información) o de la gestión de las TI (regulación ordenada de las capacidades de la organización en materia de Tecnologías de la Información de manera que aporten el máximo valor al negocio y misión de aquélla). Solo dos artículos de disposiciones comunes del "Título Tercero, de la gestión electrónica de los procedimientos" ofrecen algunos pocos criterios para la utilización de medios electrónicos y para la gestión electrónica. Normativas posteriores de desarrollo han venido a afianzar un edificio que, a pesar de los momentos de escasez presupuestaria, se encuentra en pleno periodo de construcción.

Sin aparente alineación con el Real Decreto 589/2005 que, como se recordará, había creado las Comisiones Ministeriales de Administración Electrónica y había subrayado el alcance amplio de los Planes Estratégicos, ya que debía abarcar todos los sistemas de información necesarios para responder a los objetivos estratégicos departamentales, a la hora de la regulación de su Comisión Ministerial de Administración Electrónica (mediante Orden DEF/1159/2010), el Ministerio de Defensa prefirió utilizar al atributo de la Seguridad de la Información para dejar fuera del ámbito competencial de la misma los Sistemas de Información para el "mando y control", los Sistemas de Información de "propósito general" que afectaran a situaciones de crisis y seguridad del Estado o los declarados "secreto" o "reservado" y, por último, el Sistema de Telecomunicaciones Militares y la Red de Área Extensa para Mando y Control Militar. De este modo, ante lo reducido de dicho ámbito, se dejó escapar una excelente oportunidad para, más allá de las tareas de mera coordinación interna definidas por el Real Decreto 589/2005, haber configurado esta Comisión Ministerial como órgano colegiado de apoyo a la alta dirección departamental en cuanto a las habilidades directivas propias del Gobierno Corporativo de las TI. Aunque la vigencia del Plan General de Actuación fijado en la Orden del Plan Director del año 2002 finalizara en enero de 2006, la disposición adicional tercera de esta Orden DEF/1159/2010 establece que *"el Plan Director CIS, que aprobará el Secretario de Estado de Defensa, en el marco de lo establecido en la Orden DEF/37/2005, de 30 de marzo, por la que se regula el proceso de Planeamiento de la Defensa, incluirá las políticas y estrategias corporativas en el ámbito de las Tecnologías de la Información, Telecomunicaciones, Seguridad de la Información y Administración*

Jesús Gómez Ruedas

electrónica del Ministerio de Defensa y sustituirá al Plan Director de Sistemas de Información y Telecomunicaciones aprobado mediante la Orden DEF/315/2002”.

Como corolario de todo ello, puede afirmarse que la interpretación realizada del cuerpo legislativo derivado de la Ley 11/2007 ha introducido un apreciable efecto de desenfoque en la “foto” de las Tecnologías de la Información del Ministerio de Defensa, generando el incalculable riesgo de actuar como un “cambio de agujas” que pudiera disociar el conjunto de la organización en ámbitos de negocios civiles y ámbitos de negocio militares, cada uno de ellos con sus propios sistemas, procesos y estructuras de TI, supuestamente independientes y escasamente coordinados e interrelacionados.

A la espera de ese proceso de revisión del Plan Director, como consecuencia de su alineación con el proceso de planeamiento de la Defensa, éste es el panorama actual de las TI en el Departamento. En un escenario de elevadísima complejidad tecnológica y de gestión, por el propio volumen del Ministerio y por su variedad de ámbitos de negocio, continúan su convivencia muchos sistemas de información heredados de la época previa al Plan Director de 2002 con algunos otros emanados de dicho Plan. Por el momento, el paradigma vigente continúa centrado en la tecnología.

La Seguridad de la Información y las Tecnologías de la Información. Estrategia Española de Seguridad

Aunque pudiera resultar paradójico en una institución que, desde hace más de 40 años, lleva dando cumplimiento a la **ley 9/1968, reguladora de los Secretos Oficiales**, y manejando información clasificada y, consecuentemente, se pueda afirmar que la protección de la información es algo consustancial a su vocación natural de defensa y seguridad, lo cierto es que el salto del soporte papel al soporte digital exige, en ésta como en cualquier otra organización, un cambio cultural. Éste es el “estado del arte” en el que se encontraba el Departamento a la hora del análisis de situación previo a la promulgación del Plan Director de Sistemas de Información y Telecomunicaciones: Asentados procesos de protección de materias clasificadas normalmente basados en soporte papel, procedimientos manuales y alejamiento y desconfianza de las, por entonces, incipientes redes informáticas.



Como ya se ha descrito, el Plan Director de Sistemas de Información y Telecomunicaciones incluyó a la Seguridad de la Información como una de sus líneas de acción y como uno de sus productos: La implantación de una Infraestructura de Clave Pública (PKI), la introducción de tarjetas inteligentes y un notable impulso al marco

Jesús Gómez Ruedas

normativo han sido algunos de los más reseñables avances originados por el Plan Director. En este sentido, hay que referir la promulgación de la **Política de Seguridad de la Información del Ministerio de Defensa**, mediante **Orden Ministerial 76/2006**; o las **normas para la aplicación de dicha Política**, promulgadas por **Instrucción 41/2010**, del Secretario de Estado de Defensa, que describen una estructura funcional; o las **normas para la Seguridad de la Información en las Personas**, publicadas por **Instrucción 9/2011**, del Secretario de Estado de Defensa. Con ello, el Departamento ha venido, y continúa, regulando las medidas de protección necesarias para salvaguardar la información corporativa que se pueda encontrar sobre cualquier tipo de soporte y siempre en atención a los riesgos existentes en cada uno de esos entornos.

Ciertamente, la protección de la información se encuentra estrechamente ligada al tratamiento y difusión de la misma por medio de las TI, pero bajo un enfoque de seguridad global como el que propugna la referida Política de Seguridad de la Información del Ministerio, no parece descabellado pensar que la Gestión de la Seguridad de la Información, ya definida mediante la norma UNE-ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información. Requisitos”, pueda adquirir en un futuro próximo una personalidad diferenciada de la gestión de servicios de TI, dado que las amenazas y los riesgos provienen tanto del entorno TI como de otros ajenos al mismo. Como siempre, a la hora de valorar esta decisión el criterio vendrá dictado por las necesidades de las unidades de negocio del Ministerio en cuanto a protección y tratamiento de su información.

Precisamente, aquellos tristes acontecimientos que se describen en las primeras líneas de este documento supusieron para la sociedad occidental el desencadenante de una nueva conciencia de protección de los activos de las organizaciones y entidades de esa esfera del mundo. En este nuevo contexto, cualquier decisión precisa de un análisis previo en el cual el estudio de las amenazas y de los riesgos constituye un elemento imprescindible. Este mismo enfoque es, como no podía ser de otra forma, el adoptado por la recientemente publicada **“Estrategia Española de Seguridad (EES)”**: *“Analizar las amenazas y riesgos a nuestra seguridad, identificar líneas de respuesta y definir mecanismos de coordinación son los objetivos centrales de esta primera Estrategia Española de Seguridad”*.

Las Tecnologías de la Información y los peligros tecnológicos se encuentran muy presentes en esta Estrategia. Muchas de las amenazas y riesgos identificados se relacionan directamente con un tratamiento deficiente de la información y, por tanto, con la insuficiente protección de la misma: Desde las más evidentes que constituyen las “ciberamenazas” a las actividades cotidianas de los ciudadanos que utilizan el “ciberespacio” de forma asidua, hasta las potenciales amenazas a las infraestructuras y redes de transporte del sistema energético derivadas de desastres naturales, ataques terroristas o

Jesús Gómez Ruedas

“ciberataques”. Como respuesta a estas amenazas adquieren especial relevancia diversas actuaciones, entre las que cabe subrayar:

- El desarrollo sistemático de procesos de análisis y gestión de riesgos.
- La debida atención a los sistemas para recuperación ante situaciones de desastre o, simplemente, de indisponibilidad de la información.
- La importancia de las actividades de formación y concienciación de los ciudadanos como elemento clave para contrarrestar estas amenazas. Es imprescindible promover una cultura de prevención entre los ciudadanos: Como indica la EES, *“vivir en una sociedad moderna requiere unas actitudes, aptitudes y conocimientos a un nivel hasta ahora desconocidos. Es necesario promover una mayor cultura de seguridad e impulsar la educación de los profesionales de sectores muy diversos y, en general, de los ciudadanos, en estas materias”*. Es decir, tal y como quedaba explicitado al tratar de los actuales modelos de gestión de servicios de TI, ya no es suficiente la mera ordenación de recursos para obtener el fruto esperado de las inversiones en TI: hacen falta capacidades, capacidades que, en buena parte, residen en las personas y en la forma que éstas tienen de organizarse y de trabajar (es decir, la organización y los procesos).

No cabe duda que hoy día los espacios virtuales constituyen el espacio natural donde se desarrolla una parte significativa de la actividad económica mundial. Si se desea sostener esa evolución, es imprescindible proteger los servicios de la sociedad de la información y mantener y aumentar la confianza de los ciudadanos en dichos servicios. De otro modo, la falta de seguridad de la información manejada terminaría por desestabilizar el citado entorno económico.

Balance y nuevos rumbos para tiempos de crisis

A la hora de “iluminar” con matices más ricos y coloristas este mapa de las Tecnologías de la Información del Ministerio de Defensa, algunos otros elementos merecerían un análisis detallado:

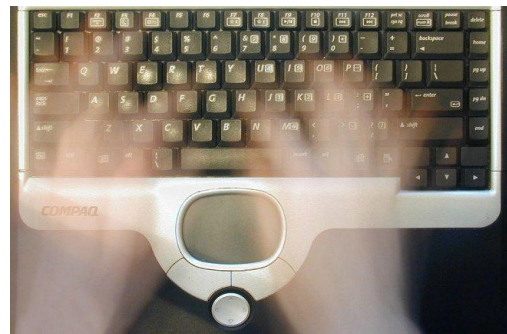
- El marco de trabajo para la gestión de los riesgos relacionados con TI, como componente fundamental de un sistema de control interno y “nudo gordiano” imprescindible para las actividades de gobierno y gestión de servicios de TI.
- Los complejos modelos descentralizados que este Ministerio despliega en materia de gestión de Recursos Humanos, de formación y capacitación del personal de TI y de proyección profesional del mismo.

Jesús Gómez Ruedas

- El difícil matrimonio entre las necesidades de los múltiples departamentos de TI del Ministerio y los procesos de contratación pública donde, regidos por la intrincada Ley 30/2007 de Contratos del Sector Público, convergen exigencias y obligaciones de adquisición de grandes volúmenes de equipamiento, por el propio tamaño de la corporación, mezclados, frecuentemente, con la provisión de servicios o la adquisición o alquiler de licencias bajo variados y no siempre sencillos modelos de licenciamiento, con singulares figuras como la Encomienda de Gestión,...
- La externalización de servicios de TI como, por ejemplo, las experiencias preliminares de la Administración Pública norteamericana para externalizar sus servicios de correo electrónico bajo un modelo privado de “computación en la nube” (Cloud Computing).
- Las modernas tendencias tecnológicas donde confluyen, entre otros, la virtualización de plataformas que pretende obtener la mayor rentabilidad de las inversiones realizadas; la imparable movilización de los terminales corporativos, que persigue tener la información siempre disponible; los desafíos que en materia de seguridad TI suponen todas estas tendencias; los retos en eficiencia energética y medioambiental; etc.

Temas críticos, cruciales y apasionantes que, para no agotar en exceso al amable lector, quedan aplazados para futuras citas.

Indudablemente, cuando solo dos mil millones de personas, sobre una población de siete mil millones, son usuarios de internet... cuando se incrementa, día a día, la población joven naturalmente predispuesta al cambio tecnológico... cuando las redes de banda ancha constituyen uno de los elementos esenciales para la nueva Economía del



Conocimiento... parece necesario mirar atrás solo el tiempo imprescindible para extraer las lecciones que depararon los éxitos y los fracasos cosechados y, rápidamente, mirar al futuro con optimismo, energías y determinación. Como dijera el escritor francés Anatole France, “**el porvenir es un lugar cómodo para colocar los sueños**”. El Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa constituyó, en su época, una acertada e innovadora iniciativa, pero el paso del tiempo y la frenética evolución de esta dinámica Sociedad del Conocimiento arrugaron su piel y su discurso. Transcurrida ya una década desde la “botadura” de aquel moderno y reformador proyecto, parece buen momento para largar amarras y, ayudados por el aprendizaje y las experiencias adquiridas durante ese periodo, elaborar **una nueva “Orden de Operaciones”**:

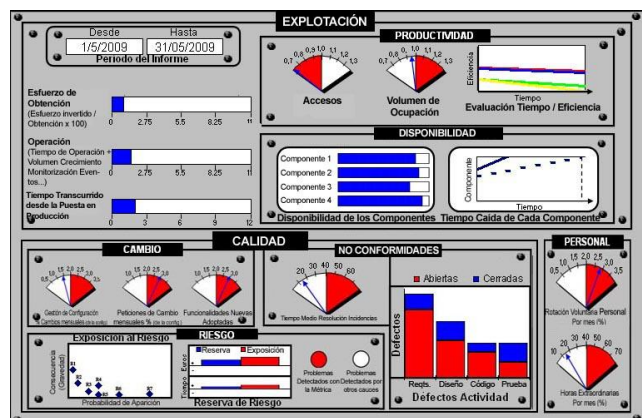
Que el Plan Director constituyera una propuesta moderna y reformista fue posible, no solo gracias al esfuerzo de todos aquellos que participaron en su planeamiento y ejecución, sino,

Jesús Gómez Ruedas

también, por el decidido e imprescindible impulso de los dirigentes del Departamento, sin el cual no habría sido posible esta visionaria acción de modernización de las Tecnologías de la Información corporativas. El liderazgo político resulta clave para vencer la resistencia al cambio.

Como posteriormente señalara con gran acierto, aunque, tal vez, con excesiva timidez, la ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, en su artículo 34, “la aplicación de medios electrónicos a los procedimientos, procesos y servicios irá siempre precedida de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio”. Quiere ello decir que la simple aplicación de soluciones tecnológicas sobre procesos de negocio que se encuentren en el mismo estado de madurez que precedía a la actual “era de la información” desvanece, sobremanera, la potencia, el efecto multiplicador y la naturaleza de elemento de valor diferencial que suponen las TI; por el contrario, prácticas de este tipo convierten a las TI en meras herramientas de mecanización que no solo no aportan un retorno a la inversión efectuada, sino que se convierten en elementos de apreciable coste y de limitado impacto para las misiones del conjunto de la organización. Probablemente, éste fuera uno de los hándicaps que mermaran con más intensidad la eficacia del Plan Director, ya que sus gestores debieron afrontar una organización estructuralmente articulada en base a procesos de negocio cuyos modelos de gestión son dispersos en ocasiones, descentralizados en otras, distribuidos a veces y, raramente, únicos y de carácter corporativo; el personal, la logística o la seguridad son claros ejemplos de esta realidad que cercena buena parte de las potencialidades de las TI en el marco del Ministerio de Defensa. En respuesta a este complejo escenario los gestores de tecnología siempre podrían sentir la tentación de reordenar, revisar y simplificar los propios procesos de negocio del Departamento por medio de “sus” Sistemas de Información: En tal caso la resistencia al cambio y el mantenimiento del statu quo establecido harían inviable esta iniciativa de “apalancar” aquéllos por medio de las TI.

Ya desde la propia directiva 336/2000, si bien de forma temporal hasta la aprobación del Plan Director, se infería el establecimiento de una estructura orgánica de Tecnologías de la Información solo en el ámbito de las Fuerzas Armadas, sin entrar a identificar tales roles y responsabilidades en el entorno de los órganos administrativos que auxilian a los órganos superiores del Departamento, es decir, Ministro y Secretarios de Estado. Como bien señalaba el



Jesús Gómez Ruedas

Vicealmirante Cayetano y Garrido, en su Documento de Opinión IEEE 02/2011 “Reflexiones Orgánicas”, el conjunto de personas, procesos de trabajo, estructuras organizativas, tecnología y entorno de actividad permite caracterizar e identificar a una organización; si sus procesos de trabajo o sus estructuras no estuvieran perfectamente integrados y vertebrados, tampoco lo estaría la propia organización, poniendo en peligro, de este modo, su operatividad y sembrando dudas sobre la eficiencia de los procesos de gestión de Tecnologías de la Información asociados a dicho modelo. Así pues, la idea de disociar las TI del Ministerio según el ámbito de negocio soportado, segregando los de carácter estrictamente operativo del resto, habitualmente del entorno de la gestión, y esbozando una imaginaria independencia o ausencia de interrelaciones entre ambos, introduce serios riesgos para la eficacia y eficiencia de la corporación.

Aun constituyendo la informática y las comunicaciones una ciencia novel y, simultáneamente, en constante y rápida evolución, del mismo modo que no parecen discutibles las prerrogativas, capacidades, misiones o autoridad de, por ejemplo, el Servicio Militar de Construcciones en lo que respecta a su natural ámbito de competencia, resulta imprescindible impulsar y consolidar un definitivo cambio cultural en el conjunto de toda la organización que haga posible la implantación de un moderno modelo de gestión de servicios de Tecnologías de la Información. En él, todos los actores deberán conocer su papel: como se pide un servicio, como se controlan los niveles de cumplimiento del servicio, como se modifica un servicio, etc.

Los actuales modelos de referencia y de buenas prácticas para el gobierno y la gestión de servicios TI nacieron, o se consolidaron, con posterioridad a la preparación y publicación del Plan Director del Ministerio; pasados unos pocos años han acrecentado su madurez y su utilidad en todo tipo de organizaciones del mundo desarrollado. En su derredor, no pocas comunidades profesionales se ocupan de su permanente evolución y adecuación a las necesidades de las organizaciones que los utilizan como columna vertebral de sus políticas de gobierno y de gestión de servicios. Para el Ministerio de Defensa, resulta fundamental adoptar y adaptar esos modelos. Sin un marco de gobierno corporativo de las TI, las estrategias y planes de negocio del Ministerio no se encontrarán nunca alineados con el despliegue y uso de las TI. Sin un modelo de gestión de servicios de TI los costes de



Jesús Gómez Ruedas

implantación y mantenimiento de las TI seguirán siendo de difícil trazabilidad y, por tanto, la eficiencia permanecerá como un lejano objetivo.

Como consecuencia de lo anterior, es preciso abandonar el caduco paradigma focalizado en los Sistemas de Información y Telecomunicaciones para evolucionar a los nuevos modelos de demanda y provisión de servicios de TI: Atrás quedaron los tiempos en que los directivos y autoridades de las distintas unidades de negocio debían ocuparse del recuento de ordenadores personales como una parte de su acción de mando. Hoy día, los clientes no tienen que solicitar un ordenador para sus usuarios: deben solicitar un servicio de terminal corporativo dotado de conectividad y las aplicaciones ad-hoc precisas para el rol del usuario receptor, que, naturalmente, reemplazará al anterior que ya habrá alcanzado el final de su ciclo de vida perfectamente gestionado. Aquellos directivos y autoridades se liberarán, de este modo, de los riesgos asociados a las antiguas responsabilidades de adquisición, mantenimiento y demás actividades de gestión de componentes TI.

Parece bastante razonable definir e implantar un único Centro de Servicios de TI, de alta especialización y cualificación, como proveedor de servicios para toda la corporación; necesitará aglutinar los actuales recursos segregados actualmente en más de una decena de centros de producción e identificar su adecuado dimensionamiento en razón a los servicios demandados por la extensa y variada lista de clientes corporativos. Dicho Centro de Servicios debería ordenar sus recursos para desplegar dos tipos de capacidades: por un lado la prestación de servicios a instalaciones permanentes dentro y fuera de Territorio Nacional, con la definición de los correspondientes Niveles de Servicio, y, por otro, una capacidad de proyección de servicios de TI allende nuestras fronteras en las zonas de operaciones de las unidades militares. Aunque compleja en su gestión, por la propia diversidad y extensión de las misiones del Ministerio de Defensa, ésta parece la aproximación más eficaz y más eficiente en costes, siempre con la mente puesta en una perfecta y natural integración de las TI en los procesos de negocio de la corporación. Ciertamente, un Centro de Servicios TI de este tipo debería articularse conforme a los modelos y marcos de referencia internacionales en materia de gestión TI, de modo que resultara posible la obtención de aquellas certificaciones que fueran de aplicación; dichas certificaciones tendrían el efecto beneficioso de acreditar ante los contribuyentes el uso adecuado y eficaz que el Ministerio de Defensa hace de los recursos públicos que se le asignan.

Parece también conveniente recapacitar acerca de la naturaleza del proceso de adaptación de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, al entorno de una organización de seguridad y defensa como es el caso de este Ministerio. Naturalmente, esta corporación no puede abstraerse del cumplimiento de la Ley, pero

Jesús Gómez Ruedas

tampoco hay que ignorar que los servicios directos al ciudadano no se encuentran entre sus líneas de negocio fundamentales. De alguna manera, la denominación “Administración Electrónica” supone un sello comercial con el que el legislador ha querido subrayar su compromiso con el ciudadano por medio de una Administración Pública virtual abierta las 24 horas del día para atender sus trámites; ello no debe suponer ningún menoscabo de otros procesos de negocio tradicionales de cualquier ministerio ni, por supuesto, producir una distorsión sobre la ordenación y finalidad de los servicios de TI integrados en los mismos. En cualquier caso, de acuerdo a las citadas teorías vigentes en materia de buen gobierno corporativo, no corresponde a los técnicos y tecnólogos el papel de impulsores de la utilización de las TI en el seno de los procesos de negocio de las Administraciones Públicas; este papel corresponde a las máximas autoridades de las mismas y, ciertamente, el personal técnico tiene que esforzarse en evidenciar el valor diferenciador que supone un uso eficaz y eficiente de las TI.

Para este gran desafío, será preciso vencer las intrínsecamente humanas resistencias al cambio y consolidar el cambio cultural necesario. Las personas, cuando se trata de servidores públicos, no debieran nunca erigirse en obstáculos para el progreso y para las reformas que apuntan en dirección a la eficacia de la institución.

Con el Plan Director de Sistemas de Información y Telecomunicaciones el Ministerio de



Defensa adquirió la madurez necesaria para empezar a navegar por el dinámico e inquietante universo de las TI corporativas: La nave ya ha abandonado el muelle, los vientos han permitido hasta ahora la navegación a vela, pero, para continuar surcando los embravecidos mares de los agresivos y exigentes entornos de negocio, ahora será necesario poner el buque “a toda

máquina” para no quedar “al garete” perdidos en medio de la inmensidad del mar.

Jesús Gómez Ruedas

**Cuando menos lo esperamos, la vida nos coloca delante un desafío que pone a prueba
nuestro coraje y nuestra voluntad de cambio.**

Paulo Coelho

*Jesús Gómez Ruedas¹⁴
Teniente Coronel del Ejército
Diplomado en Informática Militar
Director de Seguridad, CISA¹⁵, CISM¹⁶, ITIL Foundation
Subdirección General de Tecnologías de la Información y Comunicaciones*

¹⁴ Las ideas contenidas en los Documentos de Opinión son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa

¹⁵ CISA: Certified Information Systems Auditor

¹⁶ CISM: Certified Information Security Manager