risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido / Recibido□ □/□/2015
Aceitação /Aceptación□ 12/6/2015

Propuesta de marco de mejora continua de gobierno TI en entidades financieras

Agustín Prieto Delgado [1], Mario Piattini Velthuis [1]

Agustin.Prieto1@alu.uclm.es, Mario.Piattini@uclm.es

1 Grupo Alarcos, Instituto de Tecnologías y Sistemas de Información, Universidad Castilla-La Mancha, 1□0□ Ciudad Real, España

DOI: 10.17013/risti.15.51-67

Resumen: Uno de los planteamientos tradicionales para definir el buen Gobierno Corporativo (GC) es conseguir alinear el gobierno de Tecnologías de la Información (TI) con el negocio; pero es necesario definir una robusta y clara estructura de GC del que el Gobierno TI forme parte indivisible. El objetivo de este artículo es proponer un Marco de Mejora Continua de GC - TI (TIMEUS) especialmente adaptado a entidades financieras.

Palabras-clave: Gobierno Corporativo (GC), Gobierno TI, Alineamiento TI con negocio, Marco de Mejora Continua de Gobierno Corporativo (TI).

Proposal for a continuous improvement IT governance framework at financial institutions

Abstract: One of the traditional approaches to define Corporate Governance (CG) is to align the government Information Technology (IT) within the business but you need to define a robust and clear GC structure which IT government formed an indivisible part. The aim of this paper is to propose a Continuous Improvement Framework CG-IT (*TIMEUS*) specially adapted to financial institutions.

Keywords*:* Corporate Governance (CG), IT Governance, IT Alignment with business, Continuous Improvement CG Framework (IT).

1. Introducción

Cada día en mayor medida las organizaciones dependen de TI para cubrir las necesidades del negocio y crecer y/o, al menos, perdurar en su actividad. Esta dependencia requiere cada vez una mayor calidad de los servicios TI y se consigue mediante unas buenas directrices de GC de las TI (Fernández □ Piattini, 2012), políticas, principios, buenas prácticas y métodos que aplicados al unísono, faciliten la mejora continua de cualquier tipo de servicio.

Existen multitud de definiciones y caracterizaciones de Gobierno de TI, entre las que destacan□

- COBIT 5: el gobierno de TI asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar los objetivos de empresa acordados y equilibrados que han de ser alcanzados; establecer la dirección mediante la priorización y toma de decisiones; y supervisando el rendimiento y el cumplimiento respecto a la dirección y objetivos acordados (ISACA, 2012)
- ITGI (IT Governance Institute): el gobierno de TI es responsabilidad del comité de dirección y de los ejecutivos. Es una parte integral del gobierno de la organización y consiste en el liderazgo y las estructuras y procesos organizativos que aseguran que las TI de la organización sostienen y extienden la estrategia y los objetivos de la organización (ITGI, 2002).
- ISO 38500: el gobierno de TI es el sistema mediante el que se dirige y controla el uso actual y futuro de la TI (ISO/IEC, 2008).
- Weill y Ross (2004) destacan que deben gobernarse: los principios de TI, la arquitectura empresarial, la estrategia, las necesidades de las aplicaciones de la organización, y la priorización de las inversiones de TI.
- Dahlberg y Kivijärvi (2006) señalan que el gobierno de las TI debe ser integral e incluir tanto los procesos de gobierno como las perspectivas de estructura, integrando las estructuras y procesos de gobierno, el alineamiento de negocio, las operaciones de TI y la medición de desempeño y la entrega de valor.
- Webb et al. (2006) consideran que el gobierno de TI es el alineamiento estratégico de TI con la organización tal que se consigue el máximo valor de negocio por medio del desarrollo y mantenimiento de un control y responsabilidades efectivas, gestión del desempeño y gestión de riesgos de TI.
- Hoogervorst (2009) define gobierno de TI como la competencia organizacional para ejercitar de manera continuada la autoridad referente (guía) sobre la estrategia y el desarrollo de la arquitectura de TI, y el consiguiente diseño, implementación y operación de los sistemas de TI. Por ello, se centra en: Estrategia y arquitectura de TI, Gestión de la cartera de proyectos y Gestión de los programas (y proyectos) de TI.

La ventaja de un buen gobierno de las TI se ha demostrado en numerosas organizaciones. Así, por ejemplo, Hardy (2006) destaca que la construcción de un sólido modelo de gobierno para las TI diseñado para asegurar la responsabilidad acerca de y la respuesta para lograr los requisitos de negocio, pueden llevar a operaciones más eficientes y efectivas, tales como:

- Mejora en el gobierno de la organización y las TI
- Mejora en la comprensión entre ejecutivos de TI y otros ejecutivos
- Mejora en la toma de decisiones debido a información más oportuna y de mejor calidad
- Iniciativas de proyectos alineados a requisitos de negocio
- Conformidad con otros requisitos reglamentarios, tales como privacidad
- Mejora en las operaciones con un enfoque integrado de seguridad, disponibilidad e integridad de proceso
- Gestión de riesgos optimizada
- Priorización más eficiente de las iniciativas de negocio y de TI.

Holt (2013) también resalta los beneficios de un buen gobierno de TI:

- Reducción de costes, incluso teniendo en cuenta que la introducción del gobierno tiene un coste asociado
- Mejora del desempeño
- Capacidad para reaccionar rápidamente a los cambios en el mercado, ya que es fácil reconfigurar los activos de TI
- Mejora en la satisfacción del cliente, las prácticas de buen gobierno ayudan a identificar quien y cómo se usan los productos
- Prácticas más sostenibles
- Aumento de los ingresos por coste monetario

Calder (2005) señala que los principales drivers del gobierno TI son□la b□squeda de la ventaja competitiva en una economía de la información cambiante de forma dinámica, los requerimientos de gobierno que evolucionan rápidamente debido a la convergencia de los mercados y regulaciones, y la necesidad de alinear los proyectos de tecnología con los objetivos estratégicos de la organización, para asegurar que entregan el valor planeado.

En este artículo vamos a defender que el alineamiento entre el Negocio y TI se tiene que replantear para asegurar un *Proceso de Mejora Continua (DAMON)* que facilite un engranaje entre ambos ya que consideramos que el gobierno TI debe ser un servicio[1] más dentro de la organización.

Para que el proceso *DAMON* posibilite un funcionamiento sin sobresalto de la corporación, debe estar presente en todos y cada uno de los procesos y estamentos del negocio. Además deben definirse unos objetivos y metas claros en el proceso *DAMON* que se puedan revisar y monitorizar conforme se evolucione.

El proceso *DAMON* estará formalmente aprobado por el Equipo Rector del Gobierno Corporativo (*ERGC*), conforme a la definición de sus roles y responsabilidades.

El buen funcionamiento y gestión del proceso *DAMON* dará lugar al Marco de Mejora Continua de GC y TI, en lo sucesivo, *TIMEUS*.

Esta propuesta del Marco de Mejora Continua de Gobierno TI está soportada por un Mapeo Sistemático de Literatura (MSL) (Genero, Cruz-Lemus □Piattini, 201□), del estado actual de Gobierno TI en banca (Prieto □Piattini, 201□) y constituye el resultado de ese trabajo.

Este artículo abarca los siguientes apartados del proceso *DAMON*□1. Introducción, 2. Descripción del proceso□□ Descripción del valor□□ Descripción de la estructura y componentes□5. Garantía del proceso y, 6. Conclusión.

2. Descripción General del Proceso *DAMON*

Presentamos, a nivel general, el proceso *DAMON* mediante la descripción de sus componentes así como de sus interrelaciones. Ver Figura 1.

[1] Servicio significa proporcionar valor a los clientes facilitándoles los resultados que quieren conseguir. Los servicios facilitan resultados mejorando el desarrollo de las tareas asociadas y reduciendo el efecto de sus limitaciones.

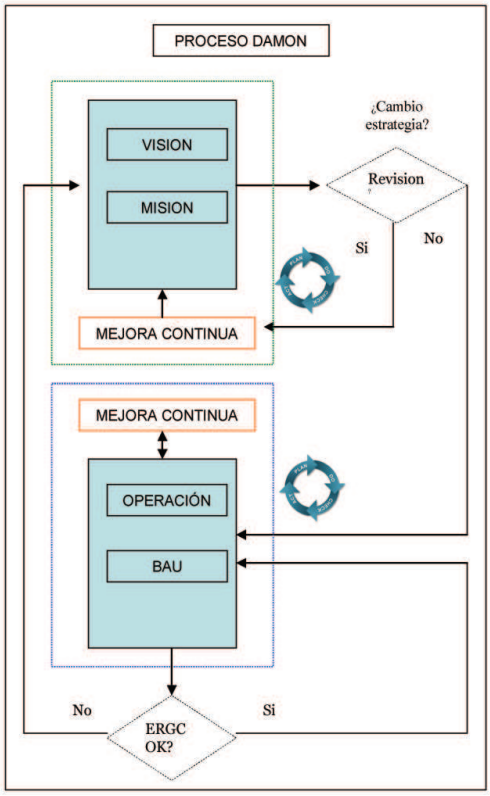

Figura 1 □Proceso *DAMON.(PDCA: Plan, Do, Check, Act)*

2.1. Alta Dirección o BoD

Mencionamos aquí la alta dirección o Board of Directors (BoD), porque conforme a la definición del ITGI (ISACA, 1998), la responsabilidad del GC y de TI, recae en este órgano.

El proceso de mejora continua *DAMON* estará formado por una representación de las áreas con más peso de la entidad y no solo por la alta dirección. Ver punto 5.6. Esta representación o grupo *ERGC*, monitorizará y ayudará a gestionar cualquier evento que pudiera cambiar o modificar la estrategia del banco (cuadro visión-misión Figura 1) o que pudiera conllevar un cambio provocado por la regulación. Además, serán los responsables de analizar, coordinar, implantar, monitorizar y gestionar el proceso *DAMON*.

Este equipo no dejará de monitorizar las entradas hasta que el proceso de mejora continua forme parte de una actividad □Business As Usual (BAU)□ (Cuadro Operación-BAU). El proceso se repite hasta que el *ERGC* esté conforme. Mejora continua en todos los procesos de la entidad. Figura 1.

3. Descripción del Valor del Proceso *DAMON*

El valor del proceso *DAMON* se basa en buscar y asegurar el alineamiento de los servicios TI con las necesidades cambiantes del negocio. El origen de los cambios del negocio pueden ser internos o externos.

Los objetivos principales del proceso *DAMON* se detallan seguidamente□

- Analizar, revisar y recomendar mejoras en cualquier fase del ciclo de vida de la estrategia de GC□diseño, transición y operación.
- Identificar e implementar actividades para mejorar la calidad, eficiencia y efectividad del GC y de TI optimizando el coste asociado.
- Proporcionar indicadores (MI).
- Reportar, a través del *ERGC*, los informes de progreso de GC.

El proceso *DAMON* proporcionará valor si□a) se comprenden los objetivos del negocio□b) hay alineamiento de la estrategia del negocio con la estrategia de TI□c) conocemos en dónde nos encontramos □situación de la organización- y hacia dónde queremos ir□personas, procesos y tecnología□d) analizamos los indicadores que nos van a permitir comprobar si se progresa adecuadamente con las distintas implementaciones de GC□e) introducimos mejoras de GC □creación *ERGC*- y, f) se incentiva la participación de la plantilla en el GC. Ver Figura 2.

4. Descripción de la Estructura y Componentes del proceso *DAMON*

4.1. Introducción

El marco de gobierno TI debe ser una pieza más de un programa de GC de la organización y está soportado por un conjunto de políticas, procedimientos, controles internos y buenas prácticas dirigidas, gestionadas y monitorizadas por la organización (Juiz □Toomey, 2015).

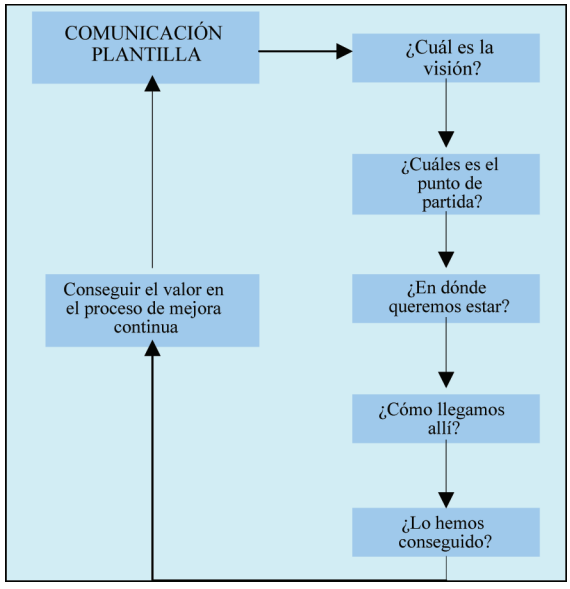

Figura 2 □Modelo de valor del proceso DAMON

La estructura de GC más habitual en la banca incluye los siguientes actores□Accionistas, Consejo de Administración y Alta Dirección.

La estructura que proponemos en este trabajo para gestionar el GC, se basa en el *ERGC* y está constituido por los siguientes miembros□un representante de la Alta Dirección, directores de las áreas de□Operaciones, TI, Cumplimiento Normativo, Asesoría Jurídica, Riesgo Operativo, Seguridad y Auditoría Interna. El *ERGC* estará formado por ocho (□) miembros y sus decisiones, acciones y actuaciones se reflejarán en actas y su actividad será auditada, al menos, una vez cada dos años por una Auditoria externa.

El *ERGC* reportará□1) al Consejo de Administración y 2) a la Alta Dirección.

4.2. Roles y responsabilidades de la estructura de dirección y gobierno más seguida en entidades financieras

Accionistas, Consejo de Administración y Alta Dirección.

El accionista es una persona física o jurídica que tiene la propiedad de acciones.

El Consejo de admón., además de sus funciones tradicionales deberá de asegurar la efectividad del Marco de Mejora Continua de GC *TIMEUS*.

La Alta Dirección, también facilitará la realización del Comité de GC□.

4.3. Roles y responsabilidades de la estructura de GC propuesta

Los tres primeros rectángulos amarillos muestran la estructura tradicional de GC.

Los siguientes dos rectángulos remarcados en rojo son claves en la estructura propuesta□ el primero, rodeado por líneas discontinuas, corresponde al *ERGC* que es el órgano director o de orquesta del marco de mejora continua del Gobierno Corporativo de entidades financieras. Validando su buen hacer, encontramos a la Auditoria Externa que se realizará al menos una vez, cada dos años. Ver Figura □

La línea siguiente de rectángulos azules, son algunos de los componentes de la dirección que forman parte del Comité *ERGC*.

Seguimos con el rectángulo de la plantilla□ese estamento es clave puesto que se le va a informar asiduamente sobre el estado de las iniciativas de GC la entidad. Además, el *ERGB* necesita su grado de satisfacción u oposición a las mismas. □stas se recogerán mediante correos enviados al *ERGB* y se analizarán y reportarán en las métricas de GC. El rectángulo violeta, indica que la plantilla tiene que tener formación obligatoria en materia de GC. Además, se pretende que la plantilla participe de todas las iniciativas de GC para que exista una total participación de todos los estamentos de la organización para alcanzar la estrategia de la entidad.

Los roles y responsabilidades de esta estructura corporativa junto al papel que desempeñarán, se detallan en la Figura □

Accionistas

Además de lo expuesto anteriormente, los accionistas serán *informados* de la constitución del *ERGC*.

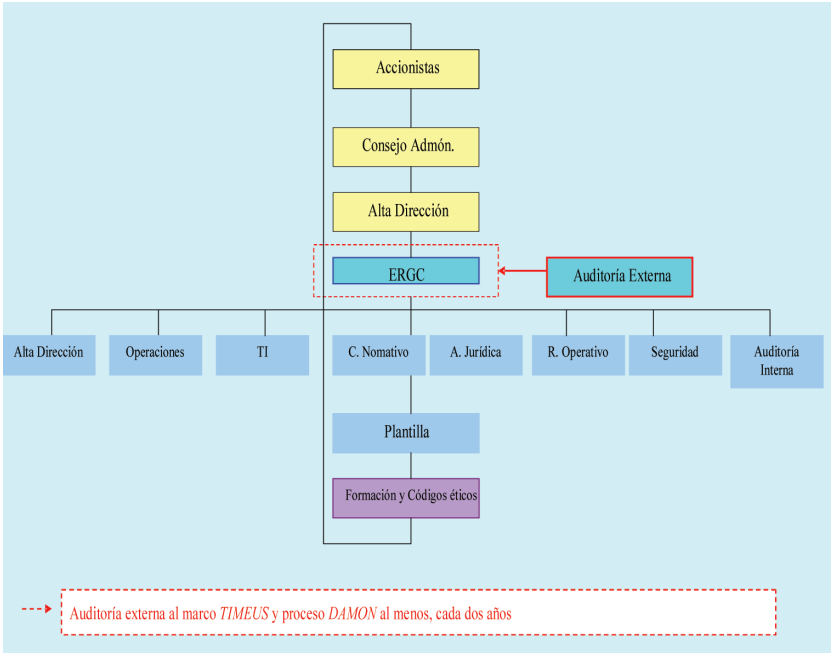

Figura □□Estructura de Gobierno Corporativo propuesta

Consejo de Administración

Además de lo mencionado anteriormente, el Consejo de Administración será el *accountable* de la constitución e informes del *ERGC*. También garantizará el funcionamiento del marco *TIMEUS* a través del cumplimiento de la política de GC, de las buenas prácticas del mercado en este ámbito a través del *ERGC* y del Comité correspondiente.

Alta Dirección

Aprobará la constitución del *ERGC* y este grupo tendrá una línea de reporte a este órgano.

Operaciones

Esta área es clave en cualquier entidad financiera ya que es la responsable de orquestar la operativa del banco así como la optimización de procesos.

La misión del director de operaciones en este grupo es valorar el impacto de las medidas de GC en la operativa del banco.

TI

Es obligada la presencia del máximo representante de TI, el CIO, en el grupo para valorar el impacto y el enfoque óptimo del área de tecnología.

Roles Responsabilidades	Accionistas	Consejo Admon	Alta Dirección	Operaciones	TI	C. Normativo	AA.JJ	R. Operativo	Seguridad	Auditoria Int	Auditoría Ext
Recibir información gestión empresa	I	A	R	I	I	I	I	I	I	C	C
Aprobación e impulso del plan estratégico	C	A	R	C	I	I	C	I	I	C	C
Aprobación operaciones societarias	C	A	R	C	I	I	C	I	I	C	C
Aprobación alianzas estratégicas	C	A	R	C	C	I	C	I	C	C	C
Control y supervisión de altos directivos	I	A/R	I	I	I	I	I	I	I	I	I
Aprobación Equipo Rector Gobierno Corporativo	I	A	R	I	I	I	I	I	I	C	I
Equipo Rector de Gobierno Corporativo (*ERGC*)											
Órganos de supervisión y control											

Figura 5. Estructura Corp. RACI (R-Resp. A-Acc. C-Cons. I- Infor)

Cumplimiento Normativo

El director de Cumplimiento Normativo conformará el grupo *ERGC* puesto que será el responsable de obtener la información, de primera mano, analizar e informar al *ERGC* de las novedades legislativas que pudieran afectar a la corporación.

Asesoría Jurídica

Desde el punto de vista de este trabajo, el director de Asesoría Jurídica formará parte del grupo *ERGC* para asesorar y evaluar el impacto de la legislación internacional y nacional, en la entidad.

Riesgo Operativo

El director de Riesgo Operativo formará parte también del *ERGC* para evaluar el impacto de posibles pérdidas por incumplimiento o retrasos en los temas relacionados con el GC.

Seguridad Corporativa

Formará parte del *ERGC* como SME (Subject Matter Expert) de cualquier tema de seguridad y de TI que pudieran afectar al GC.

Auditoria Interna

De cara a este trabajo, el director de Auditora Interna formará parte del grupo *ERGC* como parte del proceso de mejora continua y evaluadores independientes del nivel de control del GC de la entidad a través del *ERGC*.

Auditoria Externa

La Auditoria Externa se realizará concretamente para evaluación de la función del proceso *DAMON* en la actividad del GC y del marco de gobierno *TIMEUS*.

El trabajo de Auditoría Externa será solicitado, al menos, una vez cada dos años por la Alta Dirección.

5. Garantía del Proceso *DAMON*

La efectividad del proceso *DAMON* estará asegurada por el *ERGC* mediante la monitorización del cumplimiento de□

5.1. La Política de Gobierno Corporativo

La política de GC responderá siempre a la estrategia de la corporación y reflejará la declaración de intenciones de la entidad en materia de GC.

5.2. El Alineamiento de otros estándares con los puntos clave de las buenas implementaciones de Gobierno Corporativo adoptados en esta propuesta.

La propuesta del marco de mejora continua de gobierno *TIMEUS,* dará por válidos todos y cada uno de los estándares (Mesquida □Mas □San Feliu □Arcilla, 201□) reconocidos internacionalmente y sus principios estarán basados en el Estándar Internacional de Gobierno de TI ISO/IEC □□5□00. Ver Figura 5.

Este marco *TIMEUS* tendrá unos objetivos mínimos defendidos en este trabajo para las buenas implementaciones o seguimientos de GC: 1) Alineamiento estratégico, 2) Valor a través de TI, 3) Gestión del desarrollo (Mediciones), 4) Gestión del riesgo, 5) Control y accountability y 6) Regulación (Prieto & Piattini, 2015).

¿Cómo va a funcionar este alineamiento por cada una de las iniciativas de GC?

Cada una de las iniciativas de GC (Webb, Pollard & Ridley, 2006), será mapeada con los objetivos del proceso *DAMON* (cuadro verde de arriba). Por cada uno de los seis puntos que cumpla la iniciativa se dará un peso.

El cálculo de la bondad de la iniciativa se realizará por una simple regla de tres (Prieto & Piattini, 2015). Los seis (6) objetivos tenidos en cuenta en las implementaciones equivaldrían a un 100% de efectividad/bondad. Un objetivo, equivaldrá al 16%, dos, al 33%, tres, al 50%, cuatro, al 66% y cinco, al 83%.

Veamos como actuará el *ERGC* en los siguientes dos ejemplos:

1. Compra de otro banco:

Al margen del tema económico, de las due diligences y del análisis de riesgos que tienen que estar aprobados y realizados -esto quedaría fuera del alcance de este trabajo-, el *ERGC* hará el mapeo de esta iniciativa de GC con los objetivos estratégicos. Ver Figura 6.

La iniciativa de compra está alineada con la estrategia empresarial como parte de su misión. Por tanto, ya tenemos un peso en alineamiento estratégico.

En este caso en concreto, nuestra entidad (la que compra) tiene muy claro que los sistemas de información que tiene actualmente seguirán funcionando como hasta ahora. Por tanto, el valor de TI no se va a ejecutar en este caso ya que no va a aportar valor alguno desde el punto de vista de TI. No hay ningún peso. Ver Tabla 1.

Sí se va a tener en cuenta el valor del desarrollo, es decir, la entidad que compra va a medir el beneficio que los nuevos clientes van a proporcionar a la entidad. Por tanto, Gestión del Desarrollo va a tener otro peso.

Además, durante el proceso de due diligences se ha realizado una valoración del riesgo de esta operación en la entidad que compra. Esto proporcionaría otro peso adicional en este apartado.

Por último, las compras tienen que estar aprobadas por el regulador y, por tanto, sujeta a la legislación vigente. Este apartado proporcionará el último peso a la iniciativa conforme a nuestros objetivos.

El total de pesos, a alto nivel, de la iniciativa de GC -compra de otra entidad- es de cinco lo que supondría un porcentaje del 83%.

2. Auditoria externa para verificar la gestión del GC. Ver figura 6.w

La iniciativa de Auditoria externa para verificar la gestión del GC está alineada con la estrategia de la entidad puesto que existe una política de GC aprobada por

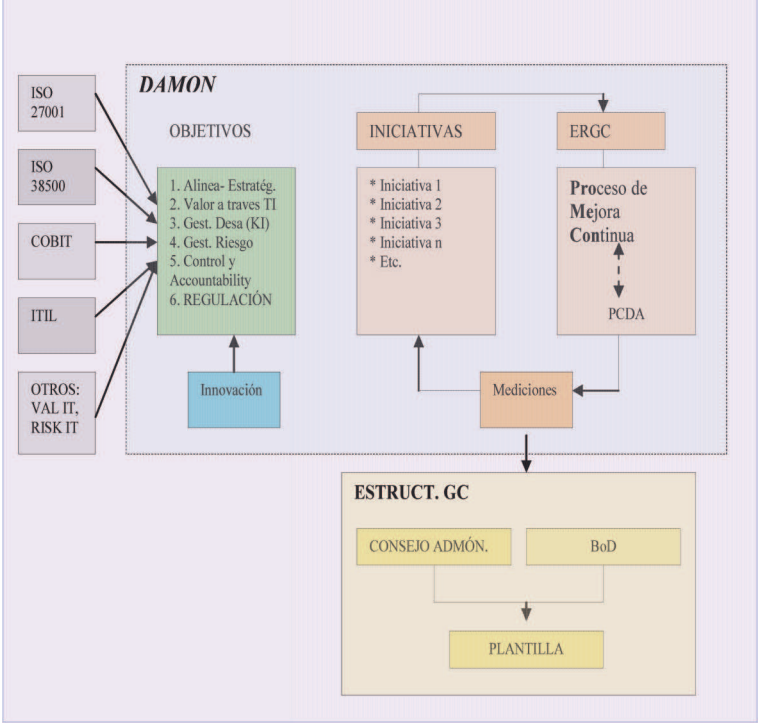

Figura 5 – Marco de Mejora de Gobierno *TIMEUS*

la dirección del banco de obligado cumplimiento para lograr una buena implementación de las iniciativas de GC. Por ello, se suma un peso al Alineamiento Estratégico. Ver tabla 1.

Como se trata de una Auditoria externa que no tiene ningún impacto en los sistemas de la entidad financiera, no asignamos ningún peso en este apartado.

Sí que va a existir una medida de un resultado del trabajo de la Auditoria que se elevará al Consejo de Administración y al BoD a través del *ERGC*. Por lo tanto, asignamos un peso a la Gestión del Desarrollo.

Los posibles puntos de la Auditoria serán asignados al responsable de su resolución junto a su fecha de cumplimiento. Esto conlleva asignar un peso en Accountability.

La Auditoria es una acción interna de la entidad financiera que no está impuesta por ninguna ley. Por ello, no asignamos ningún peso en este apartado.

El total de pesos para la iniciativa "Auditoria externa para verificar la gestión del GC" es de tres; esto significa que tenemos un porcentaje del 50%.

La misma metodología se repetirá por cada una de las iniciativas de GC y también nos servirán para tener una medida de su bondad y nivel de madurez.

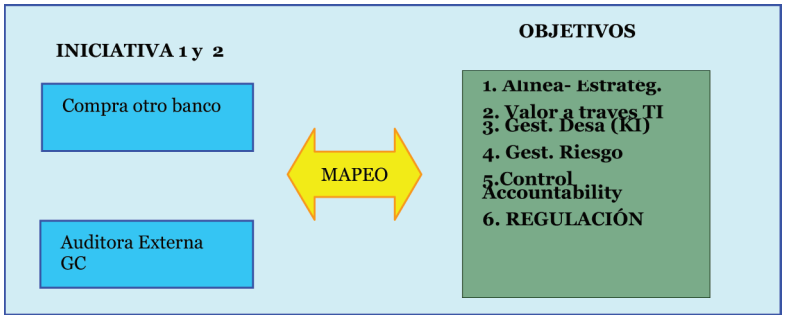

Figura 6 □Ejemplo iniciativa 1 y 2 de GC

5.3. Indicadores de Cumplimiento

Tabla 1 □Mapeo iniciativa 1 y 2 con objetivos

Iniciativa GC	Aline Estrate	Valor de TI	Gest. Desa	Gest. Riesgo	C. Accoun	Regulación	N□mero	Procentaje
Compra de otro banco	X		X	X	X	X	5	□□□
Auditoria externa para verifcar la gestión del GC	X		X		x		□	50□

Las muestras de indicadores (□I) que se reportarán por cada una de las iniciativas de seguimiento/implementación de GC en la entidad, se encuentran en la Tabla 2.

El *ERGC* será el responsable de recopilar y reportar las métricas en el Comité de GC y las informará tanto al Consejo de Administración como al BoD. Además, se definen unos umbrales por cada uno de los indicadores. Ver Figura □

Algunos de los umbrales se han definido teniendo en cuenta el número máximo de casos que la entidad financiera quiere asumir, por ejemplo, en el caso de iniciativas de GC, la entidad no pretende gestionar más de cuatro iniciativas por mes. Este n□mero es demasiado alto pero se ha definido así debido a la exigencia, cada día mayor, de requisitos de regulación.

La columna □□ltimo RAG□(Rojo, □mbar y Verde), es una información de □semáforo□para indicar cómo se han comportado los □I en el mes de la medida. Si el valor absoluto de la columna □Umbral□menos el valor absoluto de la columna □Métricas mes actual□tiene una diferencia de dos o más unidades, el RAG se pondrá en □rojo□indicando que existe una disconformidad o no cumplimiento de ese □I.

Si la diferencia entre las dos columnas mencionadas es mayor o igual que uno y menor que dos (□□1 y □2), el RAG nos mostrará un color □ámbar□para indicar que ese □I está

justo en el umbral o un poco por debajo□por ello, hay que tomar medidas correctoras para llevarlo a □verde□.El RAG verde nos indicará que ese □I está por encima del umbral. Ver Figura □

Tabla 2 □Muestra de Indicadores

Número	Indicadores
1	Aprobación Política de GC
2	Revisión Política de GC
□	N□mero incumplimientos del personal de la política GC
□	N□mero incumplimientos reincidentes
5	N□mero de iniciativas de GC
6	N□mero de iniciativas de Regulación
□	N□mero iniciativas implementadas en plazo
□	N□mero iniciativas implementadas fuera de plazo
□	N□mero de iniciativas en presupuesto
10	N□mero de iniciativas fuera de presupuesto
11	N□mero de iniciativas rechazadas
12	N□mero empleados que han completado la formación de GC
1□	N□mero de comunicaciones realizadas a la plantilla
1□	N□mero de feedback (comentarios) de la plantilla
15	N□mero de dispensas gestionadas
16	N□mero de dispensas asumido el riesgo por BoD
1□	N□mero de dispensas renovadas
1□	Ciberataques

En ese □ltimo caso, el motivo de averiguar si el valor (RAG), a□n siendo □verde□, se debe a consolidar y mejorar la madurez del proceso como mejora continua.

5.4. Planes de remediación de incumplimientos

Los planes de remediación pasan por identificar el incumplimiento, entenderlo y realizar un análisis de la causa o causas que lo han motivado.

Se diseñará un plan de acción para remediar el incumplimiento y se añadirá al registro de valoración de riesgos del área que haya ocasionado el incumplimiento.

Los planes de remediación así como su evolución se informarán en el Comité de *ERGC*. Ver Figura □

Si la remediación del cumplimiento conlleva inversión (Gomes □ Romao, 2012) o implicación de personal adicional de la entidad, será elevado al BoD por el *ERGC*. Ver Figura □

5.5. Informe de situación

El *ERGC* reportará mensualmente los avances en los seguimientos de GC de la entidad al Consejo de Administración y al BoD.

5.6. Ciclo de Deming seguido en la mejora continua del marco de gobierno *TIMEUS*

El ciclo de Deming (Deming, 1□□□), mejora y consolida las gestiones llevadas a cabo por el *ERGC* en la entidad de la siguiente manera□

1. Mejora de iniciativas de gobierno TI mediante la planificación (*Plan*).
2. Implementaciones de iniciativas de mejora de gobierno TI (*Do*).
□ Revisar el proceso globalmente (monitorizar), medirlo y comprobar que funciona de forma efectiva (*Check*).
□ Mejora integral del marco de mejora continua *TIMEUS* mediante la implementación y refinamiento de acciones (*Act)*. Ver punto 5.2.

6. Conclusiones y Futuros Trabajos

Existen escasas experiencias publicadas de implementaciones de Gobierno TI en entidades financieras y, las que hemos encontrado, están orientadas a aspectos muy concretos y no presentan un nivel de detalle suficiente para poder valorar su bondad con objetividad. Echamos en falta una medida de la madurez en esas implementaciones. Algunas de ellas están justificadas por las legislaciones locales; que obligan a seguir ciertos marcos de Gobierno TI.

La falta o deficiencia de controles robustos de GC sigue provocado escándalos en prestigiosas entidades financieras a nivel internacional y la prensa no cesa en publicarlo. Esto provoca el deterioro de su imagen desconfianza de la sociedad.

En este trabajo proponemos una estructura de GC específica basada en un órgano denominado Equipo Rector de Gobierno Corporativo (*ERGC*), constituido por una representación de todos los estamentos de la corporación. El modelo detallado presenta tres líneas de defensa□1) *ERGC*□2) representante de la alta dirección y órganos de control y, □) la plantilla.

Planificación detallada de Indicadores de Riesgo (KI)									Mes: octubre 2014
Categoría de Riesgo	Nombre KI / Descripción	Umbral	Valores Mes Actual	Frecuencia	Métrica mes actual	Evolución	Métricas mes anterior	RAG actual	Comentarios
Principios Rectores	KI 1 - % Aprobación Política de Gobierno Corporativo	≥97%	0	Anual	97%	↑	97%	Green	
	KI2 - % Revisión de la Política de Gobierno Corporativo	≥97%	0	Anual	97%	↔	97%	Green	
	KI3 - Nº Incumplimientos de la Política GC por el personal	≥95%	3	Mensual	97%	↓	98%	Green	
	KI4 - Nº de Incumplimientos de la PGC por reincidente	≥99%	2	Mensual	98%	↓	99%	Amber	
Iniciativas de Gobierno Corporativo	KI 5 - Nº Iniciativas de Gobierno Corporativo	≥96%	4	Mensual	96%	↔	96%	Green	Cuatro como máximo
	KI 6 - Nº Iniciativas de Regulación	≥95%	1	Mensual	100%	↑	96%	Green	
	KI 7 - Nº de Iniciativas implemenetadas en plazo	≥95%	3	Mensual	98%	↑	96%	Green	
	KI 8 - Nº Inciativas fuera de plazo	≥98%	1	Mensual	99%	↑	98%	Green	
	KI 9 - Nº Iniciativas en presupuesto	≥98%	3	Mensual	98%	↓	99%	Green	
	KI 10 - Nº Iniciativas fuera de presupuesto	≥97%	1	Mensual	99%	↑	97%	Green	
	KI 11 - Nº de Iniciativas rechazadas por el ERGC	≥99%	0	Mensual	99%	↔	99%	Green	
	KI 12 - Nº casos Ciberseguridad	≥99%	1	Mensual	99%	↔	99%	Green	
Formación	KI 13 - Nº Empleados que han completado la formación de GC	≥98%	2410	Semestral	96%	↑	95%	Red	Total 2500
	KI 14 - Nº de Comunicaciones realizadas a la plantilla	≥96%	1	Mensual	99%	↑	96%	Green	
	KI 15 - Nº de Feeback de la plantilla	≥96%	700	Mensual	72%	↑	70%	Red	Total 2500
Dispensas y disconformidades	KI 16 - Nº de no conformidades gestionadas	≥97%	3	Mensual	98%	↔	98%	Green	
	KI 17 - Nº de no conformidades asumidas el riesgo	≥99%	0	Mensual	99%	↔	99%	Green	
	KI 18 - Nº de no conformidades renovadas	≥99%	0	Mensual	99%	↔	99%	Green	

Figura □□Umbrales de los indicadores

El *ERGC*, tiene la responsabilidad de gestionar, en exclusiva, todas las iniciativas enmarcadas de GC y de TI, por ende. En este trabajo hemos aligerado peso al concepto de gobierno TI y enfatizado el puro GC como paraguas ya que cualquier problema en la gestión de TI no es un problema tecnológico, sino de entidad. El *ERGC* analizará las iniciativas de GC y TI y realizará una labor de mejora continua basándose en el Ciclo de Deming. El proceso de mejora continua seguido en esta propuesta se denomina *DAMON*.

El marco de mejora continua de GC en entidades financieras *TIMEUS*, será analizado y valorado por una Auditoria externa, al menos, cada dos años.

Como trabajo futuro, nos gustaría compartir la progresión en la madurez de los indicadores de este Marco de Mejora Continua de Gobierno Corporativo *TIMEUS*.

Agradecimientos

Este trabajo ha sido financiado por el proyecto GEODAS-BC (Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER, TIN2012-□□□□□C0□-01) y por el proyecto GLOBALIA (Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla La Mancha y Fondo Europeo de Desarrollo Regional FEDER, PEII11-02□1-52□□).

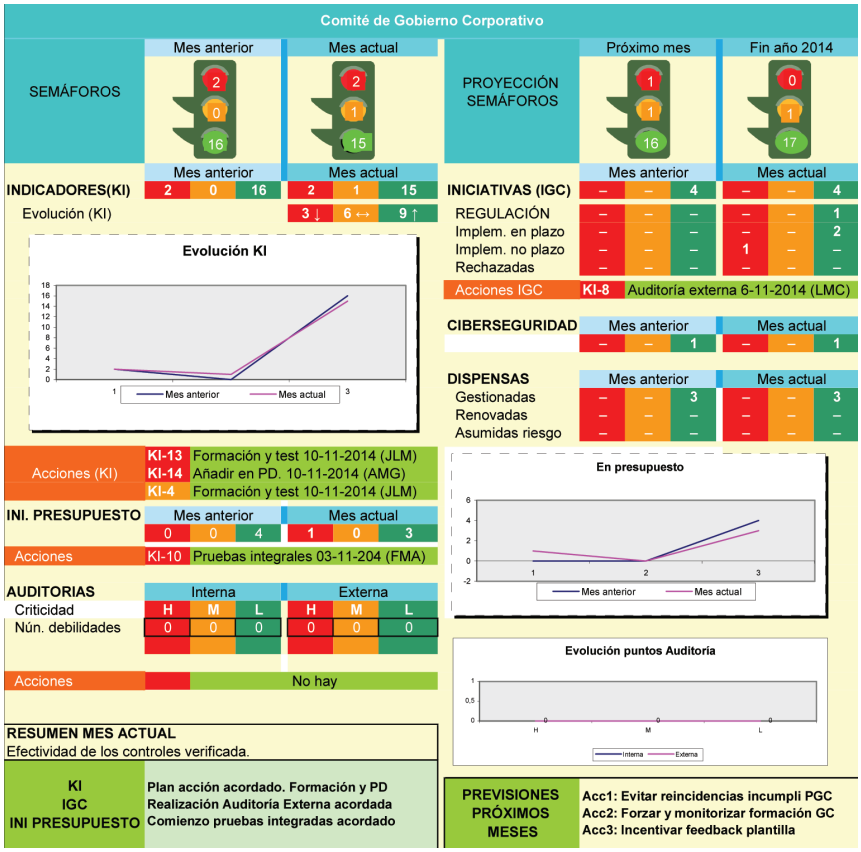

Figura □□Puntos calientes Dirección □Semáforo BoD

Referencias

Mesquida, A.L., Mas, A., San Feliu, T., Arcilla, M. (201□. Integración de Estándares de Gestión TI mediante MIN-ITs. *RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação*, (E1), □1-□5. http□//dx.doi.org/10.□□0□/risti.e1.□1-□5

Calder, A. (2005). IT Governance. Guidelines for Directors. Cambridge, U□ IT Governance Publishing.

Dahlberg, T. y □vij□ivi, H. (2006). An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. Proc. of the □□th Hawaii International Conference on System Sciences, IEEE Computer Society.

Deming, WE. (1□□□). Calidad, Productividad y Competitividad□a salida de la crisis. Ediciones Díaz de Santos (Madrid).

Fernández, CM., Piattini, M. (2012). Modelo para el gobierno de las TIC basado en las normas ISO. AENOR.

Genero, M., Cruz-Lemus, J.A., Piattini, M. (201□). Métodos de Investigación en Ingeniería del Software. □□□-□□-□□6□-50□0. RA-MA Editorial.

Gomes, J., Romão, M. (2012). Seleção de uma abordagem de gestão de investimentos em Sistemas e Tecnologias da Informação. *RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação,* (10), □5-□□ http□//dx.doi.org/10.□□0□/ristI.10.□5-50

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security Technical Report 11, 55-61.

Hoogervorst, J.A.P. (200□). Enterprise Governance and Enterprise Engineering. Diemen, Springer.

ISACA (2012). COBIT 5 Implementación. Rolling Meadows, IL, EE.UU.

ISO/IEC (200□). ISO □□5300□200□ ISO/IEC standard for corporate governance of information technology. Ginebra.

ITGI (2002). IT Governance Executive Summary, IT Governance Institute

Juiz, C., Toomey, M. (2015). To Govern IT, or not to Govern IT□ Communications of the ACM, 5□(2), 5□-6□ http□//dx.doi.org/10.11□5/2656□□5

Prieto, A., Piattini, M. (201□). Estado actual del Gobierno TI en banca. □1th Iberian Conference on Information Systems and Technologies (CISTI201□)2□66□-6□□

Webb, P., Pollard, C. y Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly□ Proc. of the □□th Hawaii International Conference on System Sciences, IEEE Computer Society.

Weill, P. y Ross, J.W. (200□). IT Governance□ How Top Performers Manage IT Decision Rights for Superior Results. Boston, MA□ Harvard Business School Press.