La norma ISO/IEC 38500 para gobierno de las TIC

Manuel Ballester, PhD IEEE, MBA, CISA, CISM, CGEIT, Cobit Trainer
Director Cátedra Buen Gobierno, Universidad de Deusto
mballester@oesia.com

Antecedentes

El Gobierno de TI (*IT Governance*) ya tiene una norma ISO asociada, la ISO/IEC 38500:2008, *Corporate governance of information technology*, que complementa el conjunto de estándares ISO que afectan a los sistemas y tecnologías de la información (*e.g.* ISO/IEC 27000, ISO/IEC 20000, ISO/IEC 15504, ISO/IEC 24762, etcétera).

Esta nueva norma fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionadas con los servicios de información y comunicación que suelen estar gestionados, tanto por especialistas en las Tecnologías de la Información y la Comunicación (TIC) internos, o ubicados en otras unidades de negocio de la organización como por proveedores de servicios externos.

En esencia, todo lo que esta norma propone puede resumirse en tres propósitos fundamentales:

- Asegurar que, si la norma es llevada a cabo de manera adecuada, las partes implicadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de TIC.
- Informar y orientar a los directores que controlan el uso de las TIC en su organización.
- Proporcionar una base para la evaluación objetiva, por parte de la alta dirección en el gobierno de las TIC.

La norma ISO/IEC 38500:2008 se publicó en junio de 2008, con base en la norma australiana AS8015:2005. Es la primera de una serie sobre normas de gobierno de TIC.

Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones los utilice al evaluar, dirigir y monitorizar el uso de las TIC. Además, está alineada con los principios de gobierno corporativo recogidos en el “Informe Cadbury” y en los “Principios de Gobierno Corporativo”, de la OCDE.

Alcance, aplicación y objetivos

La norma se aplica al gobierno de los procesos de gestión de las TIC, en todo tipo de organizaciones que utilice estas tecnologías, facilitando unas bases para la evaluación objetiva del gobierno de las TIC.

Dentro de los beneficios de un buen gobierno de las TIC, la conformidad de la organización estaría con:

- Los estándares de seguridad.
- La legislación de privacidad.
- La legislación acerca del *spam*.

- La legislación respecto a las prácticas comerciales.
- Los derechos de propiedad intelectual, incluyendo acuerdos de licencia de software.
- La regulación medioambiental.
- La normativa de seguridad y salud laboral.
- La legislación sobre accesibilidad.
- Los estándares de responsabilidad social.

También, la búsqueda de un buen rendimiento de las TIC, mediante:

- La apropiada implementación y operación de los activos de TIC.
- La clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización.
- La continuidad y sostenibilidad del negocio.
- El alineamiento de las TIC con las necesidades del negocio.
- La asignación eficiente de los recursos.
- La innovación en servicios, mercados y negocios.
- Las buenas prácticas en las relaciones con los interesados (*stakeholders*).
- La reducción de costes.
- La materialización efectiva de los beneficios esperados de cada inversión en TIC.

Definiciones

La norma incluye 19 definiciones de términos, entre los que se destacan:

- **Gobierno corporativo de las TIC** (*Corporate Governance of IT*). Sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información.
- **Gestión** (*management*). Sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización. Está sujeta a la guía y monitorización establecidas mediante el gobierno corporativo.
- **Interesado** (*stakeholder*). Individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a serlo, por una decisión o una actividad.
- **Uso de TIC** (*use of IT*). Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de TIC por unidades de negocio internas, unidades especializadas de TI, proveedores externos y *utility services* (como los que se proveen de software como servicio).
- **Factor humano** (*human behavior*). La comprensión de las interacciones entre personas y otros elementos de un sistema con la intención de asegurar el

bienestar de las personas y el buen rendimiento del sistema. Incluye la cultura, necesidades y aspiraciones de las personas como individuos y como grupo.

Principios

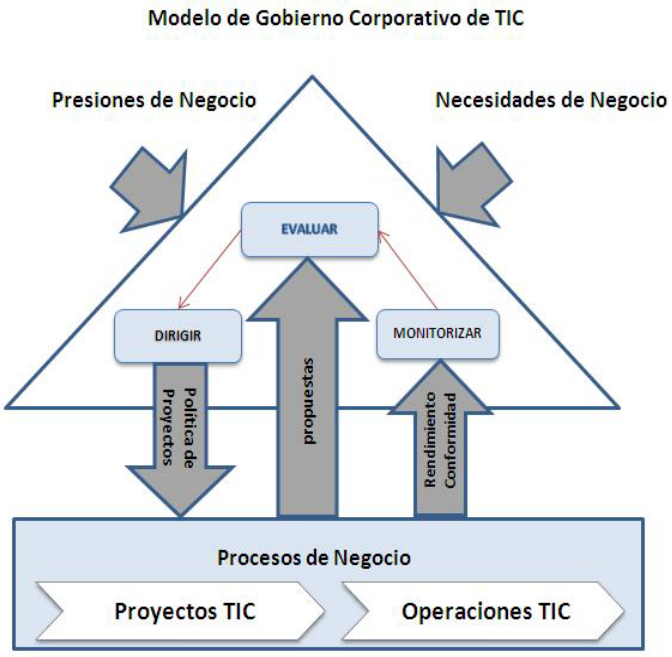
La norma define seis principios de un buen gobierno corporativo de TIC:

- **Responsabilidad**. Todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de TI. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.
- **Estrategia**. La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TIC. Los planes estratégicos de TIC satisfacen las necesidades actuales y previstas, derivadas de la estrategia de negocio.
- **Adquisición**. Las adquisiciones de TI se hacen por razones válidas, con base en un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos, tanto a corto como a largo plazo.
- **Rendimiento**. La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.
- **Conformidad**. La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.
- **Factor humano**. Las políticas de TC, prácticas y decisiones demuestran respecto al factor humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

Modelo

La dirección debe gobernar las TIC mediante tres tareas principales:

- Evaluar. Examinar y juzgar el uso actual y futuro de las TIC, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).
- Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto.
  - Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura.
  - Impulsar una cultura de buen gobierno de las TIC en la organización.
- Monitorizar. Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado.



Orientaciones y prácticas

Para cada uno de los principios, la norma proporciona una breve guía u orientación sobre cómo evaluar, dirigir y monitorizar la función de las TIC. Es decir, son orientaciones muy generales que no incluyen mecanismos, técnicas o herramientas concretas a utilizar.

Principios	Dirigir	Monitorizar	Evaluar
Responsabilidad	Planes con responsabilidad asignada	Mecanismos establecidos, gobierno TIC	Asignación de responsabilidades
	Recibir información y rendir cuentas	Asignación de responsabilidades (entendimiento)	Competencias de responsables
		Desempeño responsables del gobierno de TI	
Estrategia	Creación y uso de planes y políticas	Progreso propuestas aprobadas	Desarrollo de TIC y procesos negocio
	Asegurar beneficios TI en el negocio	Alcanzar objetivos en plazos establecidos	Evaluar actividades de TIC y alineamiento
	Alentar propuestas innovadoras	Utilizar recursos asignados	Mejores prácticas
		Uso de TIC, alcanzando los beneficios esperados	Satisfacción de interesados

			Valoración y evaluación de riesgos
Adquisición	Activos TI adquieren manera apropiada	Inversiones y capacidades requeridas	Alternativas propuestas
	Documentos capacidad requerida	Entendimiento Interno/Externo Nec. Negocio	Propuestas Aprobadas
	Acuerdos de provisión que respalden Nec. negocio		Análisis de riesgo/valor
			Inversiones
Rendimiento	Asignación recursos suficientes	Grado TIC, sustenta negocio	TIC sustenta Proc. Neg. dimensionado y capacidad
	Asignar prioridades y restricciones	Recursos e inversiones priorizados Nec. Neg.	Riesgos: continuidad operaciones
	Satisfacer Nec. Negocio	Políticas precisión datos	Riesgos: integridad información, protección Activos
	Datos correctos, actualizados, protegidos	Políticas uso eficiente TIC	Decisiones uso TIC apoyo al negocio
			Eficacia y desempeño gobierno TIC
Cumplimiento	TI cumple obligaciones, normas y directrices	Cumplimiento y conformidad (auditorías/informes)	TIC cumple obligaciones, normas y directrices
	Establecer y aplicar políticas (uso TI interno)	Oportunos, completos, adecuados (Nec. Negocio)	Conformidad gobierno TIC
	Personal TIC cumple directrices desarrollo y conducta	Actividades de TIC	
	Ética rija acciones relacionadas TIC		
Factor humano	Actividades TI compatibles factor humano	Actividades TIC, identificar, prestar atención	Actividades TIC, identificar
	Informar cualquier individuo (riesgos, problemas)	Prácticas de trabajo consistente uso apropiado TIC	Actividades TIC, considera debidamente
	Administración riesgos según políticas y procedimientos		
	Escalado a los decisores		

Beneficios y conclusión

La norma se aplica al gobierno de los procesos de gestión de las TI, en cualquier tipo de organizaciones que utilicen todas las tecnologías de la información, facilitando unas bases para la evaluación objetiva del gobierno de TI.

Dentro de los beneficios de un buen gobierno de TI estaría la conformidad de la organización con:

- Estándares de seguridad.
- Legislación de privacidad.
- Legislación sobre el *spam*.
- Legislación sobre prácticas comerciales.
- Derechos de propiedad intelectual, incluyendo acuerdos de licencia de software.
- Regulación medioambiental.
- Normativa de seguridad y salud laboral.
- Legislación sobre accesibilidad.
- Estándares de responsabilidad social.

También la búsqueda de un buen rendimiento de la TI mediante:

- Apropiada implementación y operación de los activos de TI.
- Clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización.
- Continuidad y sostenibilidad del negocio.
- Alineamiento de las TIC con las necesidades del negocio.
- Asignación eficiente de los recursos.
- Innovación en servicios, mercados y negocios.
- Buenas prácticas en las relaciones con los interesados (stakeholders).
- Reducción de costes.
- Materialización efectiva de los beneficios esperados de cada inversión en TI.