norma española

UNE-ISO/IEC 38500

Abril 2013

TÍTULO

Gobernanza corporativa de la Tecnología de la Información (TI)

Corporate governance of information technology.

Gouvernance des technologies de l'information par l'entreprise.

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO/IEC 38500:2008.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 71 *Tecnología de la información* cuya Secretaría desempeña AMETIC.

Editada e impresa por AENOR
Depósito legal: M 11247:2012

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

16 Páginas

ÍNDICE

Página

PRÓLOGO

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de tecnologías de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas de ISO/IEC.

La tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos miembros que emiten voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta norma internacional puedan estar sujetos a derechos de patente. ISO e IEC no serán responsables de la identificación de todos o parte de esos derechos de patente.

La Norma ISO/IEC 38500 fue elaborada por el organismo de normalización australiano “Standards Australia” (como AS 8015:2005) y ha sido adoptada bajo el procedimiento de “fast track”, por el comité técnico conjunto ISO/IEC JTC1, Tecnología de la Información, en paralelo con la aprobación por los organismos nacionales miembros de ISO e IEC

La Norma ISO/IEC 38500 es una norma asesora de alto nivel basada en principios. Además de proporcionar una orientación general sobre el rol del cuerpo de gobierno, alienta a las organizaciones a utilizar las normas que sean más apropiadas para reforzar su gobernanza de la TI.

En el momento de la publicación de la presente norma, el comité JTC1 continúa en el esfuerzo de desarrollo de documentos adicionales relativos a la gobernanza de la TI.

Estos documentos, que posiblemente se publicarán en el futuro como Informes Técnicos ISO/IEC, o bien como normas, se espera que traten una serie de temas, que incluirán:

– Gobernanza de proyectos que implican inversiones en TI.

– Gobernanza de la TI utilizada en las operaciones de negocios.

INTRODUCCIÓN

El objetivo de esta norma es proporcionar un marco de principios para los administradores[1)] cuando evalúen, dirijan y supervisen el uso de la Tecnología de la Información (TI) en sus organizaciones.

La mayoría de las organizaciones utilizan la TI como herramienta fundamental para el negocio, y pocas pueden funcionar eficazmente sin ella. La TI es también un factor importante en los planes futuros de negocio de muchas organizaciones.

Los gastos en TI pueden representar una parte importante de los gastos de una organización en recursos financieros y humanos. Sin embargo, a menudo no se produce el retorno esperado de esta inversión y el impacto negativo en las organizaciones puede ser importante.

Las principales razones de estos resultados negativos son dar mayor importancia a la tecnología, finanzas y aspectos de la planificación de las actividades de TI, que al contexto global del uso de la TI en el negocio.

Esta norma proporciona un marco eficaz para la gobernanza de la TI para ayudar a las personas del máximo nivel de las organizaciones a comprender y cumplir con sus obligaciones legales, reglamentarias y éticas respecto al uso que, en sus organizaciones, se hace de la TI.

El marco incluye definiciones, principios y un modelo.

Esta norma se ajusta a la definición de gobernanza corporativa publicada como un informe de la Comisión sobre los aspectos financieros de la gobernanza corporativa (el Informe Cadbury) en 1992. El Informe Cadbury también aportó la definición básica de la gobernanza corporativa en los Principios de gobernanza corporativa de la OCDE de 1999 (revisados en 2004). Se anima a los usuarios de esta norma a familiarizarse con el Informe Cadbury y los Principios de gobernanza corporativa de la OCDE.

La gobernanza es distinta de la gestión y, para evitar cualquier confusión, los dos conceptos se definen claramente en la presente norma.

Si bien esta norma está dirigida principalmente al cuerpo de gobierno, quien a su vez puede determinar que ciertas acciones sean realizadas por la dirección de la organización, también permite que, en algunas organizaciones (normalmente las más pequeñas), los miembros del cuerpo de gobierno también puedan desempeñar funciones claves en la gestión. De esta manera, se asegura que la norma sea aplicable para todas las organizaciones, desde las más pequeñas a las más grandes, independientemente del propósito, diseño y estructura societaria.

Esta norma también tiene por objeto informar y orientar a los involucrados en el diseño e implementación del sistema de gestión sobre políticas, procesos y estructuras que sostienen a la gobernanza.

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Objeto

Esta norma proporciona principios orientadores para los administradores[1)] de las organizaciones (incluyendo propietarios, miembros del consejo, directivos, socios, altos ejecutivos o similares) sobre el uso eficaz, eficiente y aceptable de la Tecnología de la Información (TI) en sus organizaciones.

Esta norma se aplica a la gobernanza 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 especialistas en TI de la organización como por proveedores de servicios externos, o unidades de negocio dentro de la organización.

1) NOTA NACIONAL: Por administrador entendemos a la persona (director, en inglés) que -solidaria o mancomunadamente- tiene la máxima responsabilidad en la empresa: Administradores Únicos o miembros del órgano rector: Consejo de Administración (Junta o Directorio, en ciertos países latinoamericanos). Ver 1.6.5.

También proporciona orientación a los que asesoran, informan, o ayudan a los administradores, entre los que se incluyen:

– altos directivos;

– miembros de los grupos que monitorizan los recursos dentro de la organización;

– especialistas externos, técnicos o de negocio, como pueden ser jurídicos o contables; asociaciones comerciales minoristas u organismos profesionales;

– fabricantes de hardware, software, comunicaciones y otros productos de TI;

– proveedores de servicios internos y externos (incluidos consultores);

– auditores de TI.

1.2 Campo de aplicación

Esta norma es aplicable a todas las organizaciones, ya sean empresas públicas o privadas, entidades gubernamentales y entidades sin ánimo de lucro. La norma es asimismo aplicable a organizaciones de todos los tamaños, desde las más pequeñas hasta las más grandes, con independencia de su grado de utilización de la TI.

1.3 Objetivos

El propósito de esta norma es promover el uso eficaz, eficiente y aceptable de la TI en todas las organizaciones por medio de:

– asegurar a las partes interesadas (incluidos clientes, accionistas y empleados) que si siguen la norma, pueden confiar en la gobernanza corporativa de la TI dentro de la organización;

– informar y orientar a los administradores sobre el gobierno del uso de la TI en su organización; y

– proporcionar una base de referencia para la evaluación objetiva de la gobernanza corporativa de la TI.

1.4 Beneficios de la utilización de esta norma

1.4.1 Observaciones generales

Esta norma establece principios para el uso eficaz, eficiente y aceptable de la TI. Asegurando a aquellas organizaciones que el seguimiento de estos principios ayudará a sus administradores a sopesar los riesgos y fomentar oportunidades derivadas de la utilización de la TI.

Esta norma establece un modelo de gobernanza de la TI. El riesgo de que los administradores no cumplan con sus obligaciones se mitiga prestando la debida atención al modelo y aplicando correctamente los principios.

La norma proporciona un vocabulario para la gobernanza de la TI.

1.4.2 Cumplimiento de la organización

La adecuada gobernanza corporativa de la TI puede ayudar a los administradores a asegurar el cumplimiento con las obligaciones (reglamentarias, legislativas, de derecho consuetudinario y contractuales) relativas al uso aceptable de la TI.

Sistemas inadecuados de TI pueden exponer a los administradores al riesgo de no cumplir con la legislación. Por ejemplo, en algunas jurisdicciones, los administradores podrían ser personalmente responsables si un sistema contable inadecuado tiene como resultado el impago de impuestos.

Los procesos relacionados con la TI incorporan riesgos específicos que deben abordarse adecuadamente. Por ejemplo, los administradores podrían ser considerados responsables de infracciones relativas a:

– normas de seguridad;

– legislación sobre la privacidad;

– legislación sobre correo basura;

– legislación sobre las prácticas comerciales;

– derechos de propiedad intelectual, incluidos los acuerdos de licencia de software;

– requisitos de retención de información;

– leyes y reglamentaciones ambientales;

– legislación sobre salud y seguridad;

– legislación sobre accesibilidad;

– normas de responsabilidad social.

Utilizando las directrices de esta norma, es más probable que los administradores cumplan con sus obligaciones.

1.4.3 Desempeño de la organización

La adecuada gobernanza corporativa de la TI ayuda a los administradores a asegurar que el uso de la TI contribuye positivamente al desempeño de la organización, mediante:

– una implementación y explotación adecuada de los activos de la TI

– claridad de la responsabilidad e imputabilidad tanto para el uso como para la provisión de la TI para el logro de los objetivos de la organización

– la continuidad y sostenibilidad del negocio

– la alineación de la TI con las necesidades del negocio

– la asignación eficiente de recursos

– la innovación en los servicios, mercados, y negocios

– las buenas prácticas en las relaciones con las partes interesadas

– la reducción de los costes de una organización

– la consecución real de los beneficios aprobados para cada inversión en TI

1.5 Documentos de referencia

En esta norma se hace referencia a los siguientes documentos:

Informe de la Comisión sobre Aspectos Financieros de la Gobernanza Corporativa, Sir Adrian Cadbury, London, 1992 ISBN 0 85258 913 1
OCDE Principios de Gobernanza Corporativa, OCDE, 1999 y 2004
Guía ISO 73 2002 Gestión del riesgo. Vocabulario.

1.6 Definiciones

A los efectos de la presente norma, se aplican las siguientes definiciones.

Se espera que la organización adapte la terminología utilizada en esta norma a sus circunstancias o estructura.

1.6.1 aceptable:
Satisface las expectativas, que se han podido expresar como razonables o justificadas de las partes interesadas.

1.6.2 gobernanza corporativa:
El sistema por el cual se dirigen y controlan las organizaciones. (Adaptado de Cadbury 1992, y OCDE 1999).

1.6.3 gobernanza corporativa de la TI:
El sistema por el cual se dirige y controla el uso, actual y futuro, de la TI.

La gobernanza corporativa de la TI implica evaluar y dirigir la utilización de la TI para dar soporte a la organización y la monitorización de ese uso para lograr la consecución de los planes. Incluye la estrategia y políticas para la utilización de la TI en la organización.

1.6.4 competente:
Que posee la combinación del conocimiento, las habilidades formales e informales, la formación, los atributos de experiencia y de comportamiento, necesarios para realizar una tarea o rol.

1.6.5 administrador:
Miembro del cuerpo de gobierno más alto de una organización. Incluye propietarios, miembros del comité de dirección, socios, altos ejecutivos o similares, y los mandos autorizados por leyes o regulaciones.

1.6.6 conducta humana:
La comprensión de las interacciones entre los seres humanos y otros elementos de un sistema con la intención de asegurar el bienestar de las personas y el rendimiento de los sistemas. La conducta humana incluye la cultura, necesidades y aspiraciones de las personas como individuos y como grupos.

NOTA Con respecto a la TI, hay numerosos grupos o comunidades de personas, cada una con sus propias necesidades, aspiraciones y comportamientos. Por ejemplo, las personas que utilizan los sistemas de información podrían mostrar necesidades relacionadas con la accesibilidad y ergonomía, así como la disponibilidad y el desempeño. Personas cuya función es cambiante debido a la utilización de la TI pueden plantear necesidades relacionadas con la comunicación, formación y tranquilidad. Personas involucradas en la construcción y operación de la TI podrían mostrar necesidades relativas a las condiciones de trabajo y al desarrollo de habilidades.

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

1.6.8 inversión:
Asignación de recursos humanos, financieros y otros, con el fin de alcanzar los objetivos establecidos y otros beneficios.

1.6.9 gestión:
El sistema de controles y los procesos necesarios para alcanzar los objetivos estratégicos establecidos por el órgano de gobierno de la organización. La gestión está sujeta a la dirección marcada por la política y seguimiento establecidos por medio de la gobernanza corporativa.

1.6.10 organización:
Cualquier empresa, corporación, gobierno, organización sin ánimo de lucro u otra entidad legalmente constituida que cuenta con administración y misión propias, incluyendo asociaciones, clubes, sociedades, agencias gubernamentales, empresas que cotizan en bolsa, empresas privadas y empresas unipersonales.

1.6.11 política:
Declaraciones claras y medibles de la dirección y conductas preferidas para condicionar las decisiones que se toman dentro de la organización.

1.6.12 propuesta:
Compilación de los beneficios, costes, riesgos, oportunidades y otros factores aplicables a las decisiones a adoptar. Incluye casos de negocio.

1.6.13 recursos:
Personas, procedimientos, software, información, equipos, consumibles, infraestructura, capital y fondos de maniobra, y tiempo.

1.6.14 riesgo:
Efecto de la incertidumbre sobre la consecución de los adjetivos (ISO/IEC Guide 73).

NOTA Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

1.6.15 gestión del riesgo:
Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (ISO/IEC Guide 73).

1.6.16 parte interesada (*stakeholder*):
Persona u organización que puede afectar, estar afectada, o percibir que esté afectada por una decisión o actividad (adaptado de ISO/IEC Guide 73).

1.6.17 estrategia:
Plan global de desarrollo de una organización que describe el uso eficaz de recursos en apoyo a las actividades futuras de la organización. Comprende el establecimiento de objetivos y la propuesta de iniciativas de actuación.

1.6.18 uso de la TI:
La planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de la TI para satisfacer las necesidades del negocio. Incluye la demanda y la prestación de servicios de TI por las unidades internas de negocio, unidades especializadas de TI, o proveedores externos.

2 MARCO PARA LA GOBERNANZA CORPORATIVA DE LA TI

2.1 Principios

Esta sección establece seis principios de gobernanza corporativa de la TI. Los principios son aplicables a la mayoría de las organizaciones.

Los principios expresan el comportamiento deseable para orientar la toma de decisiones. La definición de cada principio se refiere a lo que debería suceder, pero no prescribe cómo, cuándo o por quién se pondría en práctica, ya que estos aspectos dependen de la naturaleza de la organización que los implanta. Los administradores deberían exigir la aplicación de dichos principios en su organización.

2.1.1 Principio 1: Responsabilidad

Los individuos y grupos dentro de la organización comprenden y aceptan sus responsabilidades con respecto a la demanda y al suministro de productos y servicios de la TI. Quienes tienen la responsabilidad sobre las actuaciones también tienen la autoridad para llevarlas a cabo.

2.1.2 Principio 2: Estrategia

La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de la TI; los planes estratégicos de la TI satisfacen las necesidades actuales y futuras de la estrategia de negocio.

2.1.3 Principio 3: 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.

2.1.4 Principio 4: Desempeño

La TI satisface el propósito de dar soporte a la organización, mediante la provisión de servicios, niveles de servicio y calidad de servicio requeridos para alcanzar los requisitos presentes y futuros del negocio.

2.1.5 Principio 5: Cumplimiento

La TI cumple con toda la legislación y normativas obligatorias. Las políticas y prácticas están claramente definidas, implantadas y se hacen cumplir.

2.1.6 Principio 6: Conducta humana

Las políticas de TI, prácticas y decisiones relacionadas con la TI muestran respeto hacia la conducta humana, incluyendo las necesidades actuales y futuras de todas las “personas implicadas en el proceso”.

2.2 Modelo

Los administradores deberían gobernar la TI a través de tres tareas principales:

a) **evaluar** el uso actual y futuro de la TI;

b) **dirigir** la preparación y ejecución de planes y políticas para asegurar que el uso de la TI satisface los objetivos de la organización;

c) **monitorizar** el cumplimiento de las políticas y el desempeño con relación a lo planificado.

La figura 1 muestra el modelo de gobernanza de la TI en un ciclo de tipo Evaluar-Dirigir-Monitorizar. El texto que sigue a la figura 1 explica los elementos y las relaciones representados.

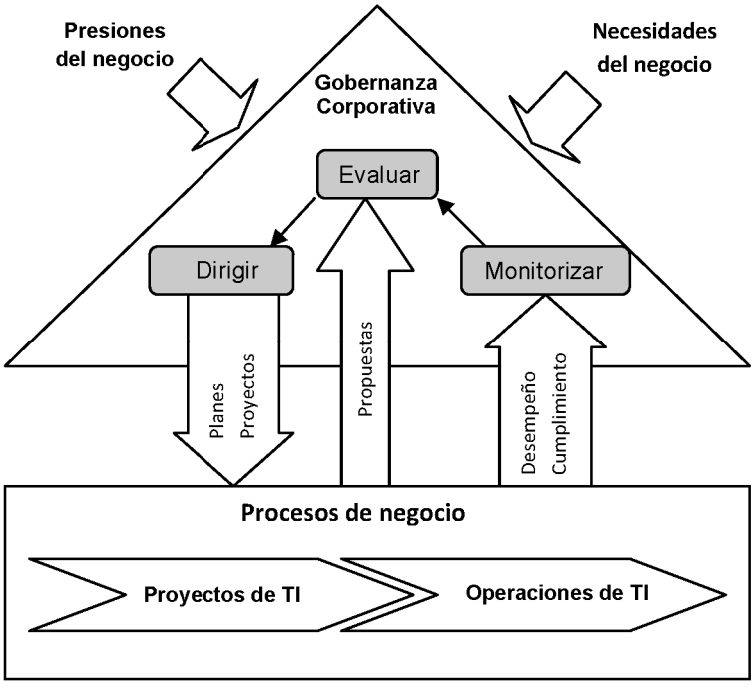

Figura 1 – Modelo de la Gobernanza Corporativa de la TI

Evaluar

Los administradores deberían valorar la situación y formular juicios sobre el uso actual y futuro de la TI, incluyendo estrategias, propuestas y acuerdos de prestación de servicios (ya sean internos, externos, o ambos).

Al evaluar el uso de la TI, los administradores deberían considerar las presiones externas o internas que actúan sobre el negocio como pueden ser los cambios tecnológicos, las tendencias económicas y sociales y las influencias políticas.

Dado que dichas influencias cambian, los administradores deberían acometer evaluaciones de forma continua.

Los administradores también deberían tener en cuenta las necesidades actuales y futuras del negocio, los objetivos organizativos actuales y futuros que deben alcanzar, tales como el mantenimiento de la ventaja competitiva, así como los objetivos específicos de las estrategias y propuestas que están evaluando.

Dirigir

Los administradores deberían asignar responsabilidades y dirigir la preparación e implantación de planes y políticas. Los planes deberían fijar el rumbo de inversiones en proyectos y operaciones de TI. Las políticas deberían establecer una conducta responsable en el uso de la TI.

Los administradores deberían asegurar que la transición de los proyectos a un estado operativo se planifique y gestione adecuadamente, teniendo en cuenta el impacto en el negocio y las prácticas operativas, y los sistemas e infraestructura de TI existentes.

Los administradores deberían fomentar una cultura de gobernanza de la TI en su organización, exigiendo a la dirección que suministre puntualmente la información adecuada, con el fin de cumplir con los objetivos establecidos y ajustarse a los seis principios de gobernanza.

Si fuera necesario, los administradores deberían controlar la presentación de propuestas a aprobar para responder a las necesidades identificadas.

Monitorizar

Los administradores deberían monitorizar el desempeño de la TI, a través de sistemas de medición adecuados. Deberían asegurarse de que dicho desempeño esté en conformidad con los planes, en particular con respecto a los objetivos de negocio.

Los administradores deberían también asegurar que la TI cumple con las obligaciones externas (normativa, legislación, derecho consuetudinario, contractuales) y las prácticas internas de trabajo.

NOTA La responsabilidad sobre aspectos específicos de la TI dentro de la organización puede ser delegada a la dirección. Sin embargo, son los administradores quienes retienen la responsabilidad final (imputabilidad) en la entrega y uso eficaz, eficiente y aceptable de la TI, la cual no puede ser delegada.

3 DIRECTRICES PARA LA GOBERNANZA CORPORATIVA DE LA TI

3.1 Observaciones generales

Los siguientes apartados ofrecen orientación sobre los principios generales de la gobernanza de la TI y las buenas prácticas necesarias para implantación de dichos principios.

Las prácticas descritas no son exhaustivas pero proporcionan un punto de partida para la discusión sobre las responsabilidades de los administradores con relación a la gobernanza de la TI. Es decir, que las prácticas descritas son una guía orientativa para la gobernanza de la TI.

Es responsabilidad de cada organización, de manera individual, la identificación de las medidas necesarias para implementar los principios, considerando debidamente la naturaleza de la organización y el análisis adecuado de los riesgos y oportunidades en el uso de la TI.

A modo ilustrativo, las prácticas descritas son aplicables a la mayoría de organizaciones (grandes o pequeñas) en la mayoría de las ocasiones. Cualquier variación debería ser considerada adecuadamente.

3.2 Principio 1: Responsabilidad

Evaluar

Los administradores deberían evaluar cuáles son las opciones existentes a la hora de asignar responsabilidades relacionadas con el uso actual y futuro de la TI en la organización. Al evaluar dichas opciones, los administradores deberían buscar el uso eficaz, eficiente y aceptable de la TI, en apoyo de los actuales y futuros objetivos de negocio.

Los administradores deberían evaluar la competencia de aquellos a quienes dieron la responsabilidad de tomar decisiones sobre la TI. En general, estas personas deberían ser directores de negocio que también son responsables de los objetivos y el desempeño organizativos, asistidos por expertos en TI que comprenden el valor y los procesos de negocio.

Dirigir

Los administradores deberían dirigir con el objetivo de que los planes se lleven a cabo de acuerdo con las responsabilidades asignadas a TI.

Los administradores deberían dirigir con el fin de recibir la información que necesitan para cumplir con sus responsabilidades y rendir cuentas.

Monitorizar

Los administradores deberían monitorizar que se hayan establecido los mecanismos adecuados de gobernanza de la TI apropiados.

Asimismo, deberían monitorizar que aquéllos a los que se les hayan asignado responsabilidades, las entienden y las asumen.

Los administradores deberían monitorizar el desempeño de aquellos a los que se les hayan asignado responsabilidades relacionadas con la gobernanza de la TI (por ejemplo, las personas que forman parte de comités de dirección o presentan propuestas a los administradores).

3.3 Principio 2: Estrategia

Evaluar

Los administradores deberían evaluar la evolución de la TI y los procesos de negocio para asegurar que la TI proporcionará apoyo a las futuras necesidades de la organización.

Al examinar los planes y las políticas, los administradores deberían evaluar las actividades de TI para asegurar que están alineadas con los objetivos de la organización ante circunstancias de cambio, que tienen en cuenta las mejores prácticas y satisfacen otros requisitos de los principales interesados.

Los administradores deberían asegurar que el uso de la TI está sujeto a una adecuada evaluación y valoración del riesgo, tal como se describe en las normas internacionales y nacionales más relevantes.

Dirigir

Los administradores deberían dirigir la creación y uso de planes y políticas que aseguren que la organización se beneficia del desarrollo en la TI.

Los administradores también deberían alentar la presentación de propuestas de usos innovadores de la TI, que permitan a la organización responder a nuevas oportunidades o desafíos, mejorando los actuales procesos de negocio o emprendiendo otros nuevos.

Monitorizar

Los administradores deberían monitorizar el progreso de las propuestas de TI aprobadas, para asegurar que alcanzan los objetivos en los plazos establecidos, utilizando los recursos asignados.

Los administradores deberían monitorizar el uso de la TI para asegurar que se alcanzan los beneficios esperados.

3.4 Principio 3: Adquisición

Evaluar

Los administradores deberían evaluar cuales son las opciones para proveerse de la TI que necesitan para desarrollar las propuestas aprobadas, equilibrando los riesgos y el valor económico de las inversiones propuestas.

Dirigir

Los administradores deberían dirigir para que los activos de TI (sistemas e infraestructura) se adquieran de manera apropiada, incluyendo la elaboración de documentación adecuada, al tiempo que se asegura que se obtienen las capacidades requeridas.

Los administradores deberían dirigir para que los acuerdos de provisión (ya sean internos o externos) soporten las necesidades de negocio de la organización.

Monitorizar

Los administradores deberían monitorizar las inversiones en TI para asegurar que se provean las capacidades requeridas.

Los administradores deberían monitorizar hasta qué punto la organización y los proveedores mantienen y comparten el propósito de la organización al realizar una adquisición de TI.

3.5 Principio 4: Desempeño

Evaluar

Los administradores deberían evaluar los medios propuestos por la dirección para asegurar que la TI sustentará los procesos de negocio con las capacidades y aptitudes requeridas. Estas propuestas deberían incluir la continuidad de la operación normal de la organización y la gestión de los riesgos asociados al uso de la TI.

Los administradores deberían evaluar los riesgos para la continuidad del negocio derivados de las actividades de TI.

Los administradores deberían evaluar los riesgos para la integridad de la información y la protección de los activos de TI, incluyendo la propiedad intelectual y la memoria colectiva de la organización.

Los administradores deberían evaluar opciones para asegurar la eficaz y oportuna toma de decisiones relativas al uso de la TI para alcanzar los objetivos del negocio.

Los administradores deberían evaluar periódicamente la eficacia y el desempeño del sistema de gobernanza de la TI de la organización.

Dirigir

Los administradores deberían asegurar la asignación de recursos suficientes para que la TI satisfaga las necesidades de la organización, de acuerdo con las prioridades acordadas y las restricciones presupuestarias.

Los administradores deberían dirigir a los responsables para asegurar que, cuando sea necesario por razones de negocio, la TI proporciona soporte al negocio con información actualizada, correcta y protegida ante pérdidas o usos inadecuados.

Monitorizar

Los administradores deberían monitorizar el grado con el que la TI sustenta el negocio.

Los administradores deberían monitorizar el grado con el cual los recursos y presupuestos asignados son priorizados de acuerdo con los objetivos de negocio de la organización.

Los administradores deberían monitorizar cómo está de extendido el seguimiento de políticas tales como las de precisión de los datos y uso eficiente de la TI.

3.6 Principio 5: Cumplimiento

Evaluar

Los administradores deberían evaluar periódicamente el grado con el que la TI cumplen con las obligaciones relevantes (normativas, legislativas, de derecho consuetudinario, contractuales), las políticas internas, las normas y directrices profesionales.

Los administradores deberían evaluar periódicamente el cumplimiento interno de la organización con su sistema de gobernanza de la TI.

Dirigir

Los administradores deberían dirigir a los responsables para establecer mecanismos periódicos y rutinarios para asegurar que el uso de la TI cumple con las obligaciones relevantes (regulatorias, legislativas, de derecho consuetudinario, contractuales), las normas y políticas establecidas.

Los administradores deberían dirigir para que estén establecidas y se hagan cumplir las políticas que permitan a la organización satisfacer sus obligaciones internas en el uso de la TI.

Los administradores deberían dirigir para que el personal de TI cumpla las directrices relevantes en materia de desarrollo y conducta profesional.

Los administradores deberían dirigir para que la ética rija todas las acciones relacionadas con la TI.

Monitorizar

Los administradores deberían monitorizar el cumplimiento y conformidad de la TI mediante prácticas adecuadas de auditoría y emisión de informes, asegurando que las revisiones sean oportunas, completas y adecuadas para la evaluación del grado de satisfacción del negocio.

Los administradores deberían monitorizar las actividades de la TI, incluyendo la pérdida de información y de activos, para asegurar que se cumplen las obligaciones ambientales, de privacidad, de gestión del conocimiento estratégico, conservación de la memoria colectiva de la organización y otras obligaciones.

3.7 Principio 6: Conducta humana

Evaluar

Los administradores deberían evaluar las actividades de la TI para asegurar que las conductas humanas se identifican y se consideran adecuadamente.

Dirigir

Los administradores deberían dirigir para que las actividades de TI sean consistentes con la conducta humana identificada.

Los administradores deberían dirigir para que los riesgos, oportunidades, problemas y preocupaciones relacionados con el negocio puedan identificarse y sean notificados por cualquier individuo en cualquier momento. Estos riesgos deberían ser gestionados de acuerdo con las políticas y procedimientos publicados, y comunicados a los principales responsables de tomar decisiones.

Monitorizar

Los administradores deberían monitorizar las actividades de TI para asegurar que las conductas humanas identificadas siguen siendo pertinentes y que se les presta una atención adecuada.

Los administradores deberían monitorizar las prácticas de trabajo para asegurar que sean consistentes con el uso apropiado de la TI.

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032