Control y un buen gobierno de ti en las organizaciones

Antoni Bosch Pujol
Institute of Audit & IT-Governance
Director General

El Control y el Buen Gobierno de los Sistemas de Información, así como la seguridad de los mismos y la prevención de los delitos informáticos ocupan los primeros puestos de las preocupaciones de los equipos directivos, además de ser uno de los principales segmentos del sector donde se están haciendo las principales inversiones y uno de los que más está creciendo.

La formación de los equipos y, sobre todo, de la dirección en relación a las TIC, se debe abordar desde una triple visión, profundizando en el estudio de las posibilidades que brinda el desarrollo tecnológico, las obligaciones y condicionantes que implica la legislación vigente y el servicio eficiente y eficaz a la estrategia de la organización.

> ***"Saber que se sabe lo que se sabe y saber que no se sabe lo que no se sabe; he aquí la verdadera ciencia"***
> **dice un viejo proverbio chino.**

INTRODUCCIÓN

Son muchos cambios en la forma de trabajar y un reto muy grande para los colaboradores que van a formar a los futuros profesionales en las TIC. Sin embargo, este cambio de paradigma en la forma de enseñar no está exento de riesgos

Las nuevas tecnologías han obligado a cambiar la forma de trabajar, a vigilar las actividades que implican tratamiento de la información dentro del ámbito de responsabilidad de las organizaciones, pero sobre todo, ha cambiado el modo de controlar el acceso y el uso de las redes para realizar actividades.

La organización ha adquirido una responsabilidad que antes no tenía: **la de vigilar los actos del personal cuando tratan información con las TIC.**

A nadie se le escapa que el riesgo aumentará al aumentar el número de colaboradores conectados en red y el tiempo de conexión de los mismos.

Y por si fuera poco, Los adolescentes están más al corriente que sus padres y sus profesores sobre cómo funcionan las nuevas tecnologías, su índice de conocimiento de las mismas es muy superior al de los adultos en general.

Para hacer frente a esta nueva responsabilidad "in vigilando" se han de implantar medidas de seguridad tecnológicas y jurídicas simultáneamente.

Durante muchos años se ha identificado el uso de las TIC y el empleo de gran profusión de medios y herramientas con la calidad de los procesos.

Muchos desarrolladores han centrado sus esfuerzos en dotar a las aplicaciones empresariales de un gran número de posibilidades tecnológicas, dejando a veces en un segundo plano el correcto diseño de la seguridad y control de los mismos.

No ha habido una planificación previa y lejos de resolver los problemas, éstos se han agravado creándose sinergias negativas que se han realimentado.

En definitiva, hemos intentado gestionar sin habernos ni tan siquiera planteado un modelo de **"Buen Gobierno de las TIC"** o **"Gobernanza de las TIC"** o **"IT-Governance".**

EL PROBLEMA

Consciente de los crecientes riesgos de las nuevas tecnologías, la Administración ha promulgado legislación sobre privacidad y protección de datos (LORTAD en el 1992, LOPD en el 1999 y la más reciente LOPDGDD en 2019), servicios de la sociedad de la información y comercio electrónico (LSSICE en el 2002), Telecomunicaciones (2003) , Firma electrónica (2003), Ley 11/2007 de administración electrónica, etc.

Esas normas tratan de regular la conducta de las nuevas tecnologías en el uso normal de nuestros centros. Sin embargo, lejos de simplificar los procesos ha añadido complejidad y por consiguiente dificultad de gobernarlas y gestionarlas adecuadamente.

Sin embargo tenemos un déficit estructural de profesionales capaces de llevar a cabo dichas tareas agudizado con la modificación del código penal por la responsabilidad penal de las personas jurídicas y el delito informático.

Así en su preámbulo cita: *"Se regula de manera pormenorizada la responsabilidad penal de las personas jurídicas. Son numerosos los instrumentos jurídicos internacionales que demandan una respuesta penal clara para las personas jurídicas, sobre todo en aquellas figuras delictivas donde la posible intervención de las mismas se hace más evidente*

(corrupción en el sector privado, en las transacciones comerciales internacionales, pornografía y prostitución infantil, trata de seres humanos, blanqueo de capitales, inmigración ilegal, ataques a sistemas informáticos...).”

En cuanto a los menores cita: *“…Por otra parte, la extensión de la utilización de Internet y de las tecnologías de la información y la comunicación con fines sexuales contra menores ha evidenciado la necesidad de castigar penalmente las conductas que una persona adulta desarrolla a través de tales medios para ganarse la confianza de menores con el fin de concertar encuentros para obtener concesiones de índole sexual. Por ello, se introduce un nuevo artículo 183 bis mediante el que se regula el internacionalmente denominado «child grooming», previéndose además penas agravadas cuando el acercamiento al menor se obtenga mediante coacción, intimidación o engaño”*.

Y referido al delito informático: *“…se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno.*

El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.”

Los avances tecnológicos nos plantean nuevos retos y peligros pero, a la vez, abren nuevas perspectivas y posibilidades, siempre que sepamos gobernarlos adecuadamente.

CLARIFICANDO CONCEPTOS

Gobernar es mucho más que gestionar, gobernar implica tomar decisiones.

Gobernar las TIC es designar a quién le damos el poder de decidir y establecer un marco de referencia de responsabilidades para que las TIC hagan aquello que realmente esperamos que hagan.

No necesitamos conocer la mecánica para poder conducir un coche, pero sí que necesitamos conocer las normas de circulación.

No necesitamos tampoco, para comprar un coche, conocer todos los modelos existentes en el mercado, pero sí las necesidades que tenemos y las posibles opciones y extras que nos ofrecen.

Del mismo modo no necesitamos conocer todos los sistemas informáticos, plataformas y sistemas de seguridad informática existentes para implementarlos, pero sí nuestras necesidades reales.

Para Gobernar las TIC tenemos que ser capaces de responder a estas seis preguntas:

- ¿Qué decisiones he de tomar?
- ¿Quién las ha de tomar?
- ¿Quién me da la información para tomarlas?
- ¿Cómo las he de tomar?
- ¿Cuándo las he de tomar?
- ¿Cómo puedo supervisarlas y controlarlas?

LA SOLUCIÓN

Un gran número de herramientas sirven para mejorar la gestión de las TI pero solo unas pocas tienen por objetivo promover sistemas de buen gobierno de las TI, aunque, el implantar herramientas de gestión de las TI va a generar una cultura organizativa muy propicia para asumir posteriormente un sistema de buen gobierno de las TI.

La norma **ISO-38500 de buen gobierno de las TIC,** está pensada principalmente para el Consejo de Dirección, y pretende ayudar a sus miembros a obtener el máximo valor de las TI y de los recursos de información de su organización.

El estándar ofrece un marco de referencia para el gobierno eficiente de las TI, con el objetivo de que los más altos directivos de una organización comprendan y satisfagan sus compromisos legales y obligaciones éticas en relación con el uso de las TI dentro de su organización.

En realidad este estándar es útil para dos colectivos diferentes:

1. Va dirigido a la alta dirección pues les indica la manera en la que deben evaluar, dirigir y monitorizar el uso de las TI en toda la organización.

2. Pero también va dirigido a los gestores de las TI pues les informa y les guía sobre como diseñar e implementar políticas de gestión, procesos y estructuras que den soporte al gobierno de las TI.

El marco de referencia para el gobierno de las TI incluido en la ISO 38500 se compone, a su vez, de: seis principios y un modelo de gobierno. Los principios expresan cuales son los comportamientos que deben adoptarse a la hora de la toma de decisiones. Cada principio establece qué es lo que debería ocurrir. El cómo, donde o quien debe implantar dichos principios dependerá de la naturaleza de la organización.

Los seis principios propuestos son:

- **Responsabilidad**, deben establecerse las responsabilidades de cada directivo y personal de administración y servicios dentro de la empresa en relación a las TI. Cada uno debe aceptar y ejercer su responsabilidad.

- **Estrategia,** a la hora de diseñar la estrategia actual y futura de la empresa hay que tener en cuenta el potencial de las TI. Los planes estratégicos de las TI deben recoger y satisfacer las necesidades tanto a corto como a largo plazo.

- **Adquisición,** las adquisiciones de TI deben realizarse bajo criterios razonables, después de un adecuado análisis y tomando la decisión en base a criterios claros y transparentes. Debe existir un equilibrio apropiado entre beneficios, oportunidades, coste y riesgos, tanto a corto como a largo plazo.

- **Desempeño,** las TI deben dar soporte a la empresa, ofreciendo servicios y alcanzando los niveles y la calidad de los servicios requeridos.

- **Cumplimiento,** las TI deben cumplir con todas las leyes y normativas. Las políticas y los procedimientos internos deben estar claramente definidos, implementados y apoyados.

- **Componente Humano,** las políticas y procedimientos establecidos deben tener en cuenta a las personas e incluir todas las cuestiones que relacionadas con ellas que puedan influir en los procesos de la empresa: competencia individual, formación, trabajo en grupo, comunicación, etc.

La norma establece que el equipo directivo debería gobernar las TI a través de 3 acciones:

Evaluar la utilización actual y futura de las TI. Los directivos deberían examinar y tomar conciencia del estado actual y futuro de las TI, incluidas estrategias, propuestas y procedimientos establecidos (tanto interna como externamente).

Dirigir la preparación e implementación de los planes y políticas que aseguren que la utilización de las TI alcanzan los objetivos de la empresa. Los planes deberían fijar el destino de las inversiones en proyectos y operaciones de TI. Las políticas deberían establecer el nivel de servicio en la utilización de las TI.

Monitorizar, mediante un adecuado sistema de medida, la adecuación a las políticas, procedimientos y planes establecidos (tanto interna como externamente).

La norma ISO 38500 se ha convertido desde su nacimiento en el mejor referente para aquellas empresas que desean implantar sistemas de gobierno de las TI. El modelo y los principios propuestos por la norma deben contribuir a generar entre los equipos directivos la cultura necesaria para abordar la implantación de un sistema integral de gobierno de las TI.

CONCLUSIONES

Gobernar las TIC supone tomar decisiones y desarrollar mecanismos para que las TIC formen parte consustancial de nuestra estrategia de centro.

Necesitamos saber qué decisiones tomar y quién las ha de tomar, gestionar nuestro portfolio TIC, conocer el marco regulatorio y legal, saber cuánto hemos de invertir y donde, gestionar el cambio y los riesgos asociados a la tecnología.

De poco nos sirve digitalizar nuestra empresa si luego no somos capaces de preservarla gestionando adecuadamente los riesgos.