São Paulo | Brasil
Av. Brigadeiro Faria Lima, 1461 - 16° andar – Torre Sul
01452-002 São Paulo | SP
Tel.: +55 (11) 2714-6900 Fax: +55 (11) 2714-6901

www.almeidalaw.com.br

ADOPCIÓN DE BUENAS PRÁCTICAS DE GOBERNANZA CORPORATIVA COMO FORMA DE EVITAR ACCIONES DE PIRATERÍA DENTRO DE LA EMPRESA

Daniela Bárbara Marti
dbmarti@almeidalaw.com.br

Las empresas en general, sobre todo aquellas que tienen en la información uno de sus principales activos deben, mediante la adopción de buena prácticas de gobernanza corporativa, establecer una cultura de protección de la información.

La integración de conceptos y prácticas de Gobernanza Corporativa, Gerencia de Riesgos y Compliance pueden auxiliar a dichas empresas a mitigar el riesgo de fraudes, espionaje industrial, hurto o desvío de informaciones. En tal escenario la adopción de controles internos vinculados a la implementación de controles de acceso resulta una medida fundamental.

Esas acciones, además de proteger el éxito y la propia continuidad del negocio, pueden también representar una forma de aumentar el valor de mercado de las empresas y reducir su coste de acceso al capital.

Mucho se ha dicho en los últimos tiempos sobre la relación del éxito empresarial con la adopción de buenas prácticas de gobierno corporativo. Un ejemplo del resultado positivo de dicha relación fue divulgado en el año 2003 por la BOVESPA (Bolsa de Valores de São Paulo). En efecto, un estudio sobre los efectos en las empresas en función de los diferentes niveles de gobernanza corporativa de la Bolsa de Valores que ostentaban, disponible en la página web de la BM&F BOVESPA , comprobó que un impacto positivo sobre la valoración de las acciones de las empresas que migraron entre esos distintos niveles de buen gobierno corporativo, con un aumento del volumen de negociación y de la liquidez de sus acciones.

Por otro lado, aunque no se considerase positiva la relación entre gobernanza corporativa y éxito empresarial, sí se puede concluir, sin demasiado esfuerzo, que un gobierno corporativo débil, puede arruinar la empresa, especialmente, cuando se trata de empresas que tienen la información como punto fundamental del desarrollo de su negocio.

Dichas empresas deben adoptar prácticas que impidan la manipulación indebida de la información. En tal contexto, el consejo de administración de la compañía tiene un papel de extrema importancia, toda vez que es él a quien competen la definición de las directrices estratégicas para la seguridad de la información, extremo que se da, en la práctica mediante la adopción de controles internos.

Los controles internos son un conjunto de políticas y procedimiento definidos por el consejo de administración e implementados por la Directoria Ejecutiva, fruto de un plano de organización, con la finalidad de garantizar, de forma razonable, la realización de los objetivos específicos de la empresa, especialmente, en lo que se refiere a la observación del alineamiento de las acciones al direccionamiento estratégico, conceder efectividad y eficiencia en el proceso de comunicación y garantizar su adecuación con las leyes y reglamentos (sean éstos internos o externos). Es necesario resaltar que muchos escándalos corporativos ocurrieron en razón de la fragilidad del ambiente de control, especialmente, de la cualidad de los controles internos contables, como por ejemplo, los casos Enron, Worldcom y del Banco Barings.

En el caso específico de la seguridad en la información, la adopción de controles internos para la mitigación de riesgos frecuentemente pasa por la implementación de los sistemas de control de acceso. Los controles de acceso físico se refieren a los mecanismos que permiten el acceso a un determinado espacio físico, tales como un edificio o una sala, sólo a personas autorizadas. Dicho control puede obtenerse por medio de una estructura vinculada a personas (por ejemplo, personas de seguridad), a través de medios mecánicos, tales como cerraduras y claves de entrada e, incluso, con sistemas basados en tarjetas de acceso.

En el ámbito de la seguridad en la información, los controles de acceso se refieren a los procesos de autenticación, autorización y auditoría. En este contexto, el control de acceso puede entenderse como la habilidad en permitir la utilización de sistemas, archivos o información solamente por personas autorizadas. El proceso de autenticación identifica a quien accede a un determinado sistema, el de autorización, determina que un usuario autentificado pueda tener acceso y, el de auditoria, identifica las acciones del usuario durante su acceso y el tiempo de duración de ese acceso.

Dichos sistemas garantiza la confidencialidad y la integridad de las informaciones de la empresa, lo que significa que a la información únicamente accederá quien esté autorizado, y que la misma estará protegida contra la manipulación indebida, lo cual podría comprometerla, por ejemplo, por la exclusión o alteración de datos.

La seguridad en la información es de vital importancia para aquellas empresas que invierten grandes cantidades de dinero en investigación y desarrollo y necesitan impedir que esas informaciones lleguen a las manos de la competencia. No obstante, el sigilo sobre la estrategia de marketing de la empresa, futuros lanzamientos y nuevos productos, también es de extrema importancia.

La implementación de sistemas de control de acceso puede también contribuir a evitar acciones de piratería dentro de la empresa, con el presente asunto.

como por ejemplo, robo de informaciones o, por lo menos, auxiliar en la identificación de las acciones que puedan concluir en una acción de piratería, como el espionaje para la obtención de secretos industriales/comerciales y la copia no autorizada de programas e informaciones.

Para garantizar que el sistema de seguridad sea completo, el compliance interno o la adecuación con toda la regulación normativa y las políticas internas definidas por la empresa, es otra medida que debe ser implementada para el fortalecimiento de los controles internos, haciendo cumplir las directrices establecidas por la alta administración de la compañía y haciendo efectiva la cultura que se pretende implementar en el ámbito empresarial.

Antes todo cuando se ha expuesto, en relación a la seguridad de la información, la adopción de buenos padrones, prácticas y conductas de buen gobierno corporativo en la empresa y el uso de controles internos orientados a la gerencia adecuada de los riesgos, aliados a un correcto compliance interno, son medidas que tienden evitar que la empresa sea cogida por sorpresa por acciones de piratería, contribuyendo también a reducir los riesgos de resultados negativos.

El sector consultivo de Almeida Advogados se coloca a su disposición para cualquier aclaración necesaria sobre el tema abordado en este artículo, contando con un equipo especializado para la consultoría jurídica en las diversas cuestiones relacionadas