

Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS, es profesor distinguido de la Facultad de Derecho de la Universidad de los Andes, Bogotá, Colombia. Ha sido practicante e investigador sobre seguridad de la información, tecnologías de información y ciencia forense digital por más de 17 años, trabajando en diferentes industrias. Él es miembro del Subcomité de Publicaciones de ISACA. Ud. puede escribirle a Cano a: jjcano@yahoo.com.

La Inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo

La palabra “cumplimiento” se usa cada vez más, día a día, para referirse a la práctica corporativa que busca asegurar la adherencia y salvaguarda de los procedimientos y aspectos normativos; de la misma manera que se utilizan los términos “buenos hábitos” y “comportamientos corporativos” (éticos y honestos) para referirse a fortalecer la gestión de negocios, de manera clara, efectiva y eficiente. En este sentido, la función de cumplimiento está a cargo de salvaguardar las operaciones de la corporación, toda vez que ella deberá estar siempre atenta y vigilante para identificar cualquier intento de alterar el “correcto orden corporativo”, y que éstos sean intervenidos y superados según se requiera.

Esta tendencia nos advierte que las empresas de clase mundial cada vez más se exigen así mismas niveles de aseguramiento corporativo, que se sustentan en las personas y sus procesos como su referente natural para asegurar que la ejecución de sus actividades, de cara al logro de los objetivos, no se desarrolle de cualquier forma, sino ajustada a las prácticas corporativas abiertas, éticas y transparentes.

A la luz de lo anterior y dada la realidad de los escándalos de corrupción, que han surgido a nivel internacional y nacional globalmente, se hace necesario insistir en la generación de una cultura que incorpore, en su estructura de creencias y valores, estrategias que promuevan comportamientos ajustados a las buenas prácticas de reporte y control corporativo, que sean garantes de los procesos corporativos y responsables frente a los resultados globales de la compañía.

ATRIBUTOS CLAVES DE LA FUNCIÓN DE CUMPLIMIENTO

Son varias los enfoques para definir la función del Oficial de Cumplimiento u Oficial en Jefe de Cumplimiento (en inglés Chief Compliance Officer—CCO), que en una primera revisión, se advierte un rol inquisitivo o acusador frente a la observancia de las regulaciones:

Also available in English
www.isaca.org/currentissue

El Chief Compliance Officer (CCO) es un oficial corporativo a cargo de la supervisión y gestión de las cuestiones de cumplimiento dentro de una organización, asegurando, por ejemplo, que una empresa se ajusta a los requisitos legales y que, ella y sus empleados, están cumpliendo con las políticas y procedimientos internos.¹

Esta definición nos presenta un ejecutivo corporativo que considera los referentes corporativos, valida su aplicación y reporta el nivel de observancia de los mismos para determinar las brechas y riesgos que se derivan de una ejecución limitada de tales referentes. Esto es, el CCO desarrolla una función de monitoreo proactiva y preventiva, que detecta una ejecución inadecuada de las prácticas, reporta las mismas y acompaña a las áreas analizadas, para superar su condición identificada y fortalecer así, el ejercicio de autoevaluación, que debiera ser una parte inherente de los procesos y sus participantes.

De otra parte, Vicente y Da Silva se acogen a la definición de la OCEG para definir que cumplimiento es:

la adherencia a, y la capacidad de demostrar la observancia de las directivas, los requisitos definidos por la ley y las regulaciones, así como de los requisitos voluntarios, como resultado de las obligaciones contractuales y las políticas internas.²

Esta definición nos circunscribe a una figura legalista y de aseguramiento de compromisos de terceros, que no aborda a los recursos fundamentales requeridos para consolidar

prácticas asociadas con mandatos de cumplimiento obligatorio, como son la cultura y la anticipación a los riesgos que afecten la dinámica corporativa. En este sentido, al igual que lo previamente señalado, la definición está ceñida a reportes de ejecución de controles definidos en la empresa que indican un nivel de aseguramiento de procesos y dan cuenta de las evidencias que revelan el estado de mitigación de los riesgos identificados.

Los siguientes son los cinco atributos clave para desarrollar una efectiva función de cumplimiento:³

- **Autoridad.** La autoridad debe estar adecuadamente ubicada en la estructura organizacional, con un nivel de reporte que asegure su independencia y la incorporación de prácticas que ayuden a la organización a ir de un nivel de madurez al siguiente.
- **Responsabilidad.** Es su deber movilizar la ejecución del programa de cumplimiento y la implementación de la función, mientras trabaja con profesionales especializados en otras áreas, que atienden riesgos claves identificados y sus impactos.
- **Competencia.** El responsable de la función de cumplimiento debe tener las credenciales necesarias, experiencia y entrenamiento para lograr una adecuada ejecución de su papel.
- **Objetividad.** El responsable de la función de cumplimiento deberá soportar las presiones organizacionales sobre situaciones particulares, para mantener el foco en el aseguramiento de las prácticas y en el reporte de sus hallazgos a la instancia correspondiente.
- **Recursos.** Deben estar disponibles los recursos requeridos para la función, teniendo en consideración el tamaño de la organización y la naturaleza de los riesgos que enfrenta.

Estos atributos nos indican que la función de cumplimiento, sin perjuicio del ejercicio permanente de monitoreo y control, deberá posicionar un estilo de reporte y seguimiento ejecutivo, concreto y medible, que establezca un referente de madurez, de manera que las mejoras se puedan identificar a través de la interacción con las áreas de negocio.

LA FUNCIÓN DE CUMPLIMIENTO Y LA SEGURIDAD DE LA INFORMACIÓN

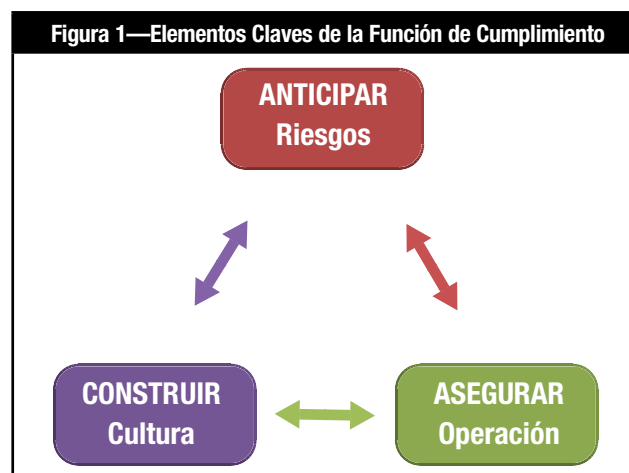
Las actividades asociadas con la función de cumplimiento, tienen en su génesis, la búsqueda de condiciones de limitación o restricción que no nos permite reforzar comportamientos y prácticas que eleven el nivel de aseguramiento de una realidad organizacional. Esto significa entender las prioridades del

negocio y su modelo de generación de valor, para liberar a la organización de la cultura de los mínimos requerimientos y movilizarla hacia la práctica de requerimientos máximos.

En este contexto, las funciones de cumplimiento se mantienen vigilantes al riesgo de no cumplimiento, que potencializan escenarios corporativos relacionados con sanciones, errores u omisiones, multas, entre otros y advierten a la empresa respecto de la aplicación sistemática de malas prácticas, que pueden terminar en incidentes que destruyan el valor de la empresa y la saquen de su ruta estratégica de mediano y largo plazo.

Considerando este argumento, en el contexto de la seguridad de la información, resulta evidente que el oficial de seguridad de la información ejerce una función de cumplimiento, que requiere los cinco atributos claves descritos previamente para lograr la transformación de los negocios y elevar el nivel de resistencia a las fallas, con una respuesta conocida frente a situaciones de excepción.

Así las cosas, cuando en el desarrollo del programa de seguridad de la información nos anticipamos a los riesgos, construimos una cultura de protección y aseguramos la operación, estamos fundando las bases de una función de cumplimiento a nivel empresarial en toda su extensión, toda vez que estos elementos buscan fortalecer comportamientos, prácticas y acciones que custodien sus resultados, salvaguarden su reputación y sobre manera, le permitan anticiparse a los eventos, haciendo que las cosas pasen. (Ver figura 1.)



La función de cumplimiento, como fuente de buenas prácticas y como sistema de monitorización activo de las

empresas, encuentra en la seguridad de la información una instancia natural de ejecución, pues al ser parte inherente del sistema de control interno de las empresas, la función de cumplimiento define recomendaciones y planes de acción que cumplen con las directrices corporativas y movilizan a la empresa hacia una cultura de debido cuidado y responsabilidad en el tratamiento de la información.

INSEGURIDAD DE LA INFORMACIÓN: EL RIESGO DE NO CUMPLIMIENTO

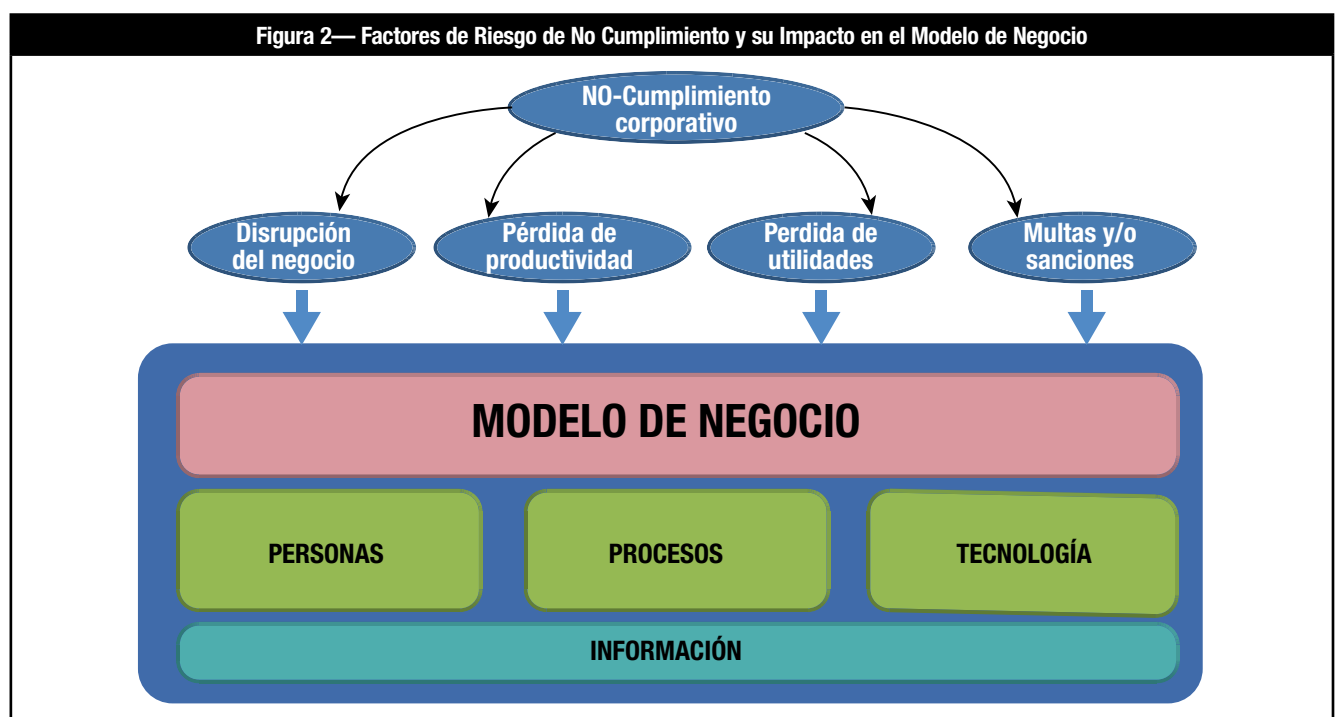
El riesgo de no cumplimiento se puede entender como la incapacidad de una organización para prevenir, detectar, corregir y mantener la comprensión de los riesgos actuales y/o emergentes, que afecten la operación empresarial y/o sus objetivos estratégicos de mediano y largo plazo. En este sentido, se hace necesario desarrollar una estrategia de tratamiento de los riesgos que permita, no solo revertir la inminencia de la materialización de los mismos, sino promover la preparación y transformación de la organización para anticiparse o visualizar la situación.

Sin importar la forma en que los métodos de administración de riesgos establezcan ciertas condiciones de ejecución, Deloitte⁴ propone un método que busca asegurar un enfoque focalizado

de tratamiento para el riesgo de no cumplimiento, siguiendo los estándares internacionales en los cuales considera aspectos como: contexto en el que ocurre, requerimientos o condiciones del riesgo, análisis del riesgo, priorización de acciones, evaluación de efectividad de controles, monitoreo, reporte y comunicación, que si bien brindan una vista que moviliza acciones concretas, no advierte la asimetría de la inevitabilidad de la falla, que se escapa al modelo causa-efecto propio de la administración de riesgos tradicional.

En este contexto, el riesgo de no cumplimiento, entendido como un factor clave en la seguridad de la información, exige desarrollar la competencia de ver desde las posibilidades de falla, las relaciones estructurales entre la tecnología, los procesos y las personas para condensar escenarios de potenciales amenazas que muestren acciones que anticipen situaciones de excepción, y no solamente adviertan el incumplimiento normativo inherente a los hechos, sino que construya la capacidad de pronóstico que le debe asistir, frente a su contexto de negocio y la responsabilidad frente a sus grupos de interés. (Ver **figura 2.**)

Por tanto, la inseguridad de la información es el concepto base desde donde se entiende el riesgo de no cumplimiento, como referente dual que invita a la empresa a encontrar en



la práctica cotidiana, patrones emergentes de malas prácticas que pueden erosionar con el tiempo la posición privilegiada de la empresa en un sector. Esto es, incubar un evento de mayor magnitud, que siendo una amenaza predecible, pase desapercibido frente a las matrices de riesgos, toda vez que no se manifiesta de manera concreta ni advierte un peligro evidente.

Cuando se entiende el riesgo de no cumplimiento más allá de sólo ajustarse a las condiciones normativas tanto interna como externas de una organización, le damos paso a una vista estructural y sistémica que permite a la empresa entender y evidenciar las leyes ocultas de la economía, la psicología y el relacionamiento de su sector de negocio, potenciando sus habilidades para identificar disruptores o agentes no identificados que cambien la manera de hacer negocios en su propio sector.⁵

REFLEXIONES FINALES

Reflexionar sobre la función de cumplimiento y su relación con las prácticas de seguridad de la información es redundar sobre las capacidades requeridas por una empresa para diferenciarse de su competencia y asegurarse una posición privilegiada en su entorno de negocio. La función de cumplimiento exige de su ejecutivo principal (CCO) quebrar el patrón de la realidad circundante, para encontrar en la interconexión de procesos, conocimiento, tecnologías de información y herramientas, tendencias emergentes que anticipen sus estrategias para avanzar en aquello donde es valioso para sus clientes y grupos de interés.

Si bien la función de cumplimiento está asociada con una vista reducida de sujeción al contexto normativo y promoción de una cultura de integridad y ética, es importante entender que dicha función debe comprender cómo la empresa crea, captura y protege el valor, para que reforzando sus capacidades y sensores del entorno, pueda continuar satisfaciendo las necesidades de sus clientes, aún cuando las mismas varíen a lo largo del tiempo.

En consecuencia y entendida la función de seguridad de la información como una aplicación natural del cumplimiento empresarial, se hace necesario caminar por los senderos de la inseguridad de la información como referente base para establecer la *potencialidad* de los riesgos de no cumplimiento, esto es, detectar los patrones futuros de las amenazas ambientales que permitan prepararla y responder a las mismas, desarrollando nuevas prácticas que generen oportunidades y factores desequilibrantes que cambien la realidad estratégica de la empresa y su entorno.

Esto implica desarrollar la capacidad de anticipación de la empresa, en términos de la inseguridad de la información, que permita identificar sinergias entre riesgos, incrementar la capacidad de monitorización, optimizar los recursos y gestiones operacionales que preparen a la empresa para actuar frente a situaciones inesperadas y se movilice de manera confiable, mientras es capaz de recuperarse frente a la falla total o parcial.

En consecuencia, la seguridad de la información como función de cumplimiento debe sintonizarse con la dinámica normal (actualidad) de la organización y sus flujos de información, para asegurar las prácticas de seguridad y control propias de los riesgos actuales del negocio. Así mismo, mantener la vista en el entendimiento constante de las relaciones propias entre las operaciones, los clientes, los procesos y las metas grandes y ambiciosas de la compañía, para ver allí como se contextualiza la inevitabilidad de la falla.

Finalmente, la función de cumplimiento como garante de la gerencia en el aseguramiento de la operación, el desarrollo de la cultura de aseguramiento y el pronóstico de nuevos escenarios de riesgos, encuentra en la seguridad de la información un aliado natural que busca un espacio natural para promover cambios estructurales y alcanzar nuevos niveles de madurez en las relaciones entre personas, procesos y tecnología que vayan más allá de la adherencia a un referente normativo o informes de desviaciones de no cumplimiento.

REFERENCIAS

- ¹ TechTarget, "Chief Compliance Officer," <http://searchcio.techtarget.com/definition/CCO>
- ² Vicente, P.; M. Mira da Silva; "A Conceptual Model for Integrated Governance, Risk and Compliance," In Mouratides, H.; C. Rolland, *Advanced Information Systems Engineering. Lecture Notes in Computer Science*, Springer Verlag, 2011, p. 199-213
- ³ Girgenti, R.; T. Hedley; *Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global Regulated, and Digital Environment*, McGraw Hill, 2011
- ⁴ Deloitte, *The Risk Intelligent Chief Compliance Officer: Champion of Risk Intelligent Compliance*, 2012, <http://webserver2.deloitte.com.co/Doc%20ERS/No.24%20The%20Risk%20Intelligence%20Compliance%20Officer.pdf>
- ⁵ Birshan, M.; J. Kar; "Becoming More Strategic: Three Tips for Any Executive," *McKinsey Quarterly*, July 2012, www.mckinseyquarterly.com/

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2013 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org