Revista Gestão & Tecnologia
e-ISSN: 2177-6652
revistagt@fpl.edu.br
http://revistagt.fpl.edu.br/

Prácticas de seguridad de la información contable y su contribución al cumplimiento de requerimientos de gobierno corporativo

Pedro Solana-González
Doutor em Engenharia Industrial pela Universidade de Cantábria (UC). Professor Associado de Organização de Negócios na Faculdade de Negócios e Economia da Universidade UC
pedro.solana@unican.es

Karen Hackbart Souza Fontana
Mestra em Ciências Contábeis pela Universidade do Vale do Rio dos Sinos (UNISINOS)
Professora da Faculdade Cesuca INEDI
karen.hsfontana@gmail.com

Adolfo Alberto Vanti
Doutor em Administração pela Universidade de Deusto (San Sebastián-Espanha).
Professor do PPGGEO – Universidade Regional Integrada do Alto Uruguai e das Missões, URI.
Pequisador CNPQ.
adolfo.vanti@san.uri.br

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SER/OJS
Recebido em 08.02.2019
Aprovado em 25.03.2019

Resumen

Esta investigación tiene como objetivo analizar cómo las prácticas de seguridad de la información contable pueden contribuir a la exigencia de cumplimiento del gobierno corporativo. Es una investigación descriptiva y cualitativa cuya estrategia de investigación fue mediante un estudio de caso realizado en una industria metalúrgica en Rio Grande do Sul que se encuentra en el nivel 2 de gobernanza corporativa. Como técnicas de recogida de datos se utilizaron documentos y entrevistas en profundidad. Se encontró como los gerentes de las áreas de control, contabilidad, impuestos, costos/planificación, finanzas y tecnología de la información, utilizan 27 de 41 prácticas de seguridad de la información contable. Se concluye que las prácticas contribuyen al cumplimiento de las normas de gobierno corporativo al proporcionar información accesible, disponible, confiable, responsable, válida, segura, así como ayuda en la mitigación de riesgos. Además, en el análisis documental se encontró que la empresa tiene políticas de seguridad de la información, así como no tuvo salvedades de la auditoría independiente en el período analizado.

Palabras clave: Seguridad de la información; Información contable; Gobierno corporativo; Cumplimiento de las normas.

Práticas de segurança da informação contábil e sua contribuição para a governança corporativa no requisito de conformidade

Resumo

Esta pesquisa tem como objetivo analisar como as práticas de segurança da informação contábil podem contribuir para a governança corporativa no requisito de conformidade. Trata-se de uma pesquisa descritiva, qualitativa cuja estratégia de pesquisa deu-se mediante um estudo de caso realizado em uma indústria metalúrgica localizada no Rio Grande do Sul que está listada no Nível 2 de Governança Corporativa. Como técnicas de coleta de dados utilizou-se de entrevistas em profundidade e documentos. Verificou-se com os gestores das áreas de controladoria, contabilidade, fiscal, custos/planejamento, financeiro e tecnologia da informação, que a empresa utiliza 27 das 41 práticas de segurança da informação contábil. Conclui-se que as práticas utilizadas contribuem para a conformidade da governança corporativa proporcionando uma informação acessível, conforme, confiável, disponível, íntegra, responsável, válida, segura, bem como ajuda na mitigação de riscos. Em complemento, verificou-se na análise documental que a empresa possui políticas de segurança da informação, bem como não teve ressalvas da auditoria independente no período analisado.

Palavras-chave: Segurança da informação; Informação contábil; Governança Corporativa; Conformidade.

Security practices of accounting information and its contribution to the corporate governance compliance requirement

Abstract

This research has as objective to analyze security practices of accounting information can contribute to the corporate governance compliance requirement. It is a descriptive and qualitative research whose research strategy was by a case study performed in a metallurgical industry in Rio Grande do Sul that is listed at level 2 of corporate governance. As data collection techniques utilized in-depth interviews and documents. It was found how managers of the areas of accounting, accounting, tax, financial and cost/planning, information technology, use 27 of 41 information security practices. It is concluded that the practices contribute to compliance of corporate governance by providing accessible information, as available, reliable, responsible, valid, safe, as well as, help in risks mitigation. In addition, it was found in the documentary analysis that the company has information security policies, as well as the independent audit had caveats analysis period.

Keywords: Information security; Accounting Information; Corporate Governance; Compliance.

1 Introducción

La gobernanza corporativa comprende las orientaciones y métodos bajo los cuáles son gobernadas las empresas. Permite a la empresa operar con más competencia, disminuir el riesgo y ofrecer protección para las limitaciones de gestión, a fin de apoyar su crecimiento (Yousuf & Islam, 2015). Esta temática ha ganado una creciente atención en los últimos años debido a los escándalos contables que han llevado a una crisis de confianza en la práctica de la emisión de informes financieros (Mateescu, 2015; Bhasin, 2016).

Con el fin de proteger a los accionistas existen un conjunto de principios de gobierno corporativo (IBGC, 2009) entre los que destaca la conformidad (*compliance* en su acepción inglesa), debido al fortalecimiento del respeto a las normas y políticas, así como a la mitigación de riesgos (Oliveira et al., 2015).

La conformidad se puede definir como la obediencia a las normas y leyes que regulan el ambiente interno y externo (Dedonatto & Beuren, 2010). Esta obediencia, específicamente en el área contable, se da por la adopción de los estándares estipulados por el *International Accounting Standards Board* (IASB) (Jorissen, 2015; Azad et al., 2016).

El proceso de convergencia a las normas del IASB en Brasil se da por medio de las directrices emitidas por el Comité de Pronunciamientos Contables (CPC) que orientan las prácticas contables, pero para que éstas sean útiles a los usuarios deben poseer determinadas características cualitativas (Hendriksen & Van Breda, 1999; Ribeiro Filho, Lopes & Pederneiras, 2009; Iudícibus, 2010; CPC 00 R1, 2011).

En este sentido, destacan los estudios recientes sobre las características cualitativas de los estados contables por medio de métricas bajo la óptica de especialistas contables (Barbosa et al., 2015), etapas de ciclo de vida de las compañías listadas en la BM&FBovespa (Lima et al. (2008), atributos de la contabilidad gerencial en el sector de energía eléctrica (Souza et al., 2015), y normas contables y calidad de las informaciones prestadas (Jorissen et al., 2015).

Se confirma así que la información es esencial para el negocio de una organización, por lo que se recomienda que se proteja (Sêmola, 2014). En este sentido, para que los objetivos de seguridad de la información (Dhillon & Backhouse, 2000; Albertin & Pinochet, 2010; Uddin & Preston, 2015) sean atendidos se deben adoptar prácticas que relacionen las tecnologías de seguridad y el comportamiento del usuario (Bulgurcu, Cavusoglu & Benbasat, 2010; Parsons et al., 2015; Safa et al., 2015).

En este contexto, distintos estudios tratan de forma aislada los temas de seguridad de la información, las características cualitativas de la información contable y la gobernanza corporativa. La presente investigación busca la integración de estos temas y tiene como objetivo analizar cómo las prácticas de seguridad de la información contable pueden contribuir a la gobernanza corporativa mediante el cumplimiento de requisitos de conformidad.

Esta investigación está delimitada por tanto dentro del marco de Gobierno Corporativo en el cumplimiento de requisitos de conformidad. En relación con la Información Contable se investigan sus características cualitativas, y en lo que se refiere a la Seguridad de la Información se considera la ISO/IEC 27002:2013 sección 18 - Conformidad.

La presente investigación se estructura de cinco secciones, la primera se refiere a esta introducción; la segunda se aborda la fundamentación teórica; en la tercera se describe la metodología; en la cuarta sección se presenta el análisis de los resultados de la investigación; y en la quinta se exponen las consideraciones finales.

2 Fundamentación teórica

Para la fundamentación teórica de la investigación se contemplan los temas de Gobernanza Corporativa, Información Contable y Seguridad de la Información.

2.1 Gobernanza corporativa: conformidad

La gobernanza corporativa se refiere a la calidad, transparencia y fiabilidad de las relaciones con los accionistas, el consejo de administración, así como la gestión que define la autoridad y responsabilidad de cada uno en la entrega de valor sostenible para todos los *stakeholders* (Adiloglu & Vuran, 2012). Está guiada por las directrices y métodos por los cuáles las empresas son gobernadas, lo que les permite operar con más competencia y disminuir el riesgo, ofreciendo protección contra la mala gestión (Yousuf & Islam, 2015).

Para proteger a los *stakeholders* se evidencian los principios de gobernanza corporativa destinados a orientar a las autoridades en la implementación de códigos nacionales eficientes de gobernanza (Mateescu, 2015). Entre los principios de buena gobernanza (IBGC, 2009) destacada la conformidad (Dedonatto & Beuren, 2010).

En este sentido, Dedonatto y Beuren (2010) evidencian que la gobernanza corporativa *"debe asegurar a los socios o inversores la equidad, transparencia, responsabilidad por los resultados (accountability) y la obediencia a las legislaciones del país (compliance) en que está inserta"*. La conformidad se refiere al cumplimiento de las normas reguladoras, tanto en el ambiente interno como externo de la organización (Ferreira et al., 2015; Mateescu, 2015). Se considera importante en la protección, creación de valor y reputación corporativa pues la buena gobernanza exige transparencia, patrones éticos y conformidad con las normas y legislación, lo que ayuda a reducir los riesgos y preserva la imagen de la organización (Oliveira et al., 2015).

Estudios recientes evidencian la interrelación entre conformidad y gobernanza corporativa (Darounco, 2013; Gerard & Weber, 2015; Griffith et al., 2016; Turrent & Ariza, 2016). En este sentido, Darounco (2013) evalúa la contribución de los procesos de control interno y de TI a la gobernanza corporativa en relación con la conformidad. Los principales hallazgos se refieren a la falta de procesos, sistemas y controles estandarizados y sistematizados, factores determinantes para la conformidad.

Gerard y Weber (2015) analizan los resultados de ocho investigaciones y profundizan en el conocimiento sobre la gobernanza corporativa examinando las ventajas y limitaciones de la función de conformidad. Los autores destacan que la conformidad soporta la gobernanza corporativa.

Griffith et al. (2016) abordan la conformidad como *"un medio de asegurar que los funcionarios y otras partes están cumpliendo con las normas y reglamentos internos y externos de la organización"*. Los autores afirman que la conformidad posibilita la evaluación del riesgo, pero puede limitar la actividad de la empresa.

Turrent y Ariza (2016) analizan el nivel de conformidad de la gobernanza corporativa en empresas no financieras de las bolsas de Argentina, Brasil, Chile y México, en el período de 2004 – 2010, señalando una tendencia creciente de la conformidad que propicia un mayor control y sostenimiento de la reputación en el mercado.

Se constata por ello que la conformidad en la gobernanza corporativa ha sido ampliamente estudiada. En este respecto Mateescu (2015) enfatiza que la gobernanza corporativa tiene una variedad de enfoques estando relacionada con el derecho, las finanzas, la gestión y la contabilidad.

2.2 Información contable: características cualitativas

En la contabilidad la información es esencial. Ribeiro Filho, Lopes e Pederneiras (2009) afirman que el objetivo de la contabilidad es identificar, medir, registrar y divulgar las informaciones sobre la situación patrimonial, financiera y resultado de las entidades. Para Azad et al. (2016) la contabilidad se puede definir como un sistema que mide las actividades del negocio, procesando la información en los informes, haciéndolos disponibles para los tomadores de decisión a través de los estados contables.

Iudícibus (2010) destaca que los estados contables tienen como objetivo promover informaciones útiles para la toma de decisión de sus usuarios. En este sentido, la información debe poseer ciertas características cualitativas (Ribeiro Filho, Lopes & Pederneiras, 2009; CPC 00 R1, 2011) que se definen como *"las propiedades de la información que son necesarias para que sea útil"* (Hendriksen & Van Breda, 1999, p. 95).

De acuerdo con Souza et al. (2015) las características cualitativas de la información contable, también llamadas atributos de la contabilidad gerencial, agregan calidad a los informes, haciéndolos comparables a otros y fácilmente comprensibles por los accionistas y *stakeholders*.

La Figura 1 se presenta la revisión de la literatura y estudios empíricos sobre las principales características cualitativas de la información contable.

Características	Descripción	Autor/año
Comparabilidad	Permitir al usuario identificar diferencias y similitudes.	Hendriksen y Van Breda (1999); Ribeiro Filho, Lopes y Pederneiras (2009) Iudícibus (2010); CPC 00 R1 (2011); Souza et al. (2015); Jorissen (2015); Azad et al. (2016)
Comprensibilidad	Debe ser expuesta en la forma más comprensible al usuario.	
Confiabilidad	El usuario acepta la información y la utiliza como base de la toma de decisión.	
Consistencia	Uso de conceptos y procedimientos de medición similares para ítems afines.	
Disponibilidad	Estar accesible a los usuarios.	
Integridad	Información lo más completa posible, sin omisión de algún hecho relevante.	
Materialidad	La omisión o la distorsión provocan una influencia en las decisiones de los usuarios.	
Neutralidad	No hay sesgos.	
Oportunidad	Informaciones íntegras y oportunas.	
Predictivo	Predicción de resultados futuros.	
Primacía de la esencia sobre la forma	Refleja lo que de hecho ocurrió independientemente del contrato.	
Prudencia o conservadurismo	Cautela cuando existen incertidumbres.	
Relevancia	Capaz de hacer una diferencia en las decisiones de los usuarios.	
Representación fidedigna	Estar libre de errores, sesgos y manipulaciones.	
Oportunidad	Ofrecer información en tiempo hábil para la toma de decisión.	
Uniformidad	Los eventos iguales se representan de forma idéntica.	
Utilidad	Debe ser relevante y fiable.	
Verificabilidad	Los usuarios deben llegar a un consenso, pero no a un acuerdo.	

Figura 1 - Principales características cualitativas de la información contable
Fuente: Elaborado en base a las obras consultadas.

Para que la información contable sea útil y de calidad las características de la Figura 1. posibilitan una información esencial para la organización, por lo que se recomienda su protección (Sêmola, 2014).

2.3 Seguridad de la información

La seguridad de la información se ha convertido en un elemento esencial para las organizaciones a fin de eliminar los riesgos (Shamala et al., 2015) y de mejorar la conformidad de la información (Safa, Von Solms & Furnell, 2016). Se puede definir, conforme a Sêmola (2014, p. 41), como *"un área del conocimiento dedicada a la protección de activos de la información contra accesos no autorizados, alteraciones indebidas o su indisponibilidad"*.

El propósito de la seguridad de la información es garantizar la protección de la información contra accesos no deseados, facilitando su disponibilidad en el momento oportuno de forma confiable (Albertin & Pinochet, 2010). De este modo, está influenciada por tres

propiedades principales: la confidencialidad, la integridad y la disponibilidad de la información (Sêmola, 2014). Adicionalmente, en la Figura 2 se destacan otras importantes características relativas a la seguridad de la información.

Requisitos	Descripción	Autor/año
Conformidad	Cumplimiento de requisitos.	Sêmola (2014); Buccafurri et al. (2015); Safa, Von Solms y Furnell (2016)
Protección	Protección de la información contra accesos no deseados.	Albertin y Pinochet (2010)
Confidencialidad	Acceso y uso restringido de contenidos a las personas autorizadas.	Dhillon y Backhouse (2000); Albertin y Pinochet (2010); Sêmola (2014); Uddin y Preston (2015); Safa et al. (2015)
Integridad	Protección contra alteraciones indebidas.	
Disponibilidad	Disponible a los usuarios.	
Legalidad	Estar en conformidad con la legislación.	Albertin y Albertin e Pinochet (2010)
Conciencia	Actuación de acuerdo con las expectativas del usuario.	
Uso legítimo	Control de acceso al sistema.	
Confiabilidad	Actuación del sistema conforme a lo esperado.	
Responsabilidad	Responder con las obligaciones y afrontar nuevas oportunidades.	Dhillon y Backhouse (2000)
Confianza en el comportamiento	Estándares de comportamiento aceptados y acordados	
Ética	Comportamientos informales, valores morales.	
Políticas de seguridad	Declaraciones de papeles y responsabilidades de los empleados para salvaguardar la información y los recursos.	Bulgurcu, Cavusoglu y Benbasat (2010); Albertin y Pinochet (2010); Fontes (2012)
Autorización	Permiso para el acceso a la información.	Sêmola (2014)
Auditoría	Identificar las entidades involucradas en el intercambio de información.	
Autenticidad	Garantía de que la información no ha cambiado después de su envío o validación.	
Gravedad	Gravedad del daño que el activo puede sufrir mediante una amenaza.	
Relevancia del activo	Grado de importancia de un activo para la ejecución de un proceso de negocio.	
Relevancia del proceso de negocio	Grado de importancia del proceso de negocio para el logro de los objetivos y la supervivencia de la empresa.	
Criticidad	Gravedad relativa al impacto en el negocio causado por problemas de seguridad.	
Identificación	Identificación del emisor, autor de las informaciones.	

Figura 2 - Requisitos de seguridad de la información
Fuente: Elaborado en base a las obras consultadas.

En la Figura 2 se muestran los requisitos de seguridad de la información bajo la óptica teórica y de estudios empíricos. De este modo, para que los objetivos de seguridad de la

información (Dhillon & Backhouse, 2000; Albertin & Pinochet, 2010; Uddin & Preston, 2015) puedan ser atendidos, se deben utilizar prácticas de seguridad de la información relacionadas con la adopción de tecnologías de seguridad y el comportamiento del usuario (Bulgurcu, Cavusoglu & Benbasat, 2010; Sêmola, 2014; Parsons et al., 2015; Safa et al., 2015).

Las prácticas de seguridad de la información pueden reducir las vulnerabilidades, limitar los impactos y evitar los riesgos para el negocio (Sêmola, 2014). En este sentido, la norma ISO/IEC 27002:2013 considera específicamente las prácticas de seguridad de la información por medio de un conjunto adecuado de controles, políticas y procedimientos organizacionales y funciones de *software* y *hardware*.

De acuerdo con Sêmola (2014) la ISO/IEC 27002:2013 se constituye como un importante instrumento para las empresas preocupadas por la operación de su negocio y la protección de la información. La norma posee 18 categorías de seguridad de la información, donde cada categoría posee un objetivo de control (lo que se espera alcanzar) y las directrices para su implementación (información detallada de apoyo al control).

Se contempla en esta investigación el detalle de las prácticas referentes a los dominios constantes en la sección 18 - Conformidad. Los dominios se refieren a: Identificación de la legislación aplicable (D1); Derechos de propiedad intelectual (D2); Protección de registros organizacionales (D3); Protección y privacidad de la información de identificación personal (D4); Reglamentación de controles de criptografía (D5); Análisis crítico independiente de la seguridad de la información (D6); Cumplimiento de las políticas y procedimientos de seguridad de la información (D7); y Análisis crítico de la conformidad técnica (D8).

Se considera la conformidad como uno de los aspectos más importantes de la seguridad de la información (Sêmola, 2014).

3 Metodología

Esta investigación sigue una orientación descriptiva, por cuanto busca referir el comportamiento de los fenómenos estudiados para su análisis, de forma que se puedan identificar y obtener informaciones sobre las características y hechos relevantes de un determinado problema o cuestión (Collis & Hussey, 2005). Se utilizó como estrategia metodológica el estudio de caso, que permite al investigador una profundización en el fenómeno estudiado. En cuanto al abordaje del problema, se delinea como cualitativa, pues enfatiza los

aspectos subjetivos de la actividad humana, enfocándose en el significado del fenómeno estudiado (Collis & Hussey, 2005).

Se utilizaron como fuentes de recogida de datos entrevistas y documentos. El instrumento de recolección se compone de 41 prácticas de seguridad de la información contable (Fontana, 2017). Los entrevistados fueron 7 gestores de las áreas que se relacionan directamente con la contabilidad, ocupando los siguientes cargos: coordinador de contabilidad, coordinador fiscal, coordinador de costos/planificación, gerente de TI, supervisor de TI, gerente de control y gerente financiero. Las entrevistas fueron realizadas individualmente y grabadas, con una duración media de 1 hora 20 minutos. Las respuestas fueron transcritas y posteriormente enviadas a los gestores para su validación.

Se realizó asimismo un análisis documental para corroborar y aumentar las evidencias obtenidas en las entrevistas. Los documentos analizados fueron el Balance Patrimonial (BP), la Demostración del Resultado del Ejercicio (DRE), las Políticas y Normas internas.

La investigación se realizó en una industria metalúrgica ubicada en el Estado de Rio Grande do Sul. La elección de la empresa se tomó al cumplir los siguientes requisitos: (i) es una empresa de capital abierto, regida por las disposiciones legales y reglamentarias de la Ley nº 6.404; (ii) posee una clasificación en el Nivel 2 de Gobernanza Corporativa, (iii) es líder en su segmento de actuación en Brasil; (iv) se clasifica como gran empresa; y (v) su disponibilidad en participar en la investigación. La empresa "X", así denominada por razones de confidencialidad, tiene acciones negociadas en la BM&FBovespa desde 1982 e ingresó en el Nivel 2 de Gobernanza Corporativa en 2011.

4 Análisis de los resultados

El análisis cualitativo de las entrevistas se compone de: (i) la categorización de los entrevistados; (ii) las prácticas de seguridad de la información contable.

4.1 Categorización de los entrevistados

Los encuestados se encuentran en las siguientes áreas: Contabilidad, Costos, Financiera, Fiscal y Tecnología de la Información; que representan 7 gestores. Se constató que el 42,85% de los gestores tienen menos de 5 años en la empresa y el 57,14% tiene más de 5 años. En cuanto al nivel de escolaridad, el 100% de los gestores poseen el nivel de postgrado. Otra variable abordada se refiere al área de formación académica. Se destacan Ciencias Contables

con el 57,14% seguida de Administración de Empresas con el 28,57% y Tecnología de la Información con el 14,28%.

4.2 Prácticas de seguridad de la información contable

Las cuestiones de investigación se refieren a los 8 dominios (D) de la norma ISO/IEC 27002:2013 sección 18, integrados con las características cualitativas de la información contable y con los requisitos de conformidad de la gobernanza corporativa que totalizan 41 prácticas. Se constató la utilización de 27 prácticas de seguridad de la información contable. A continuación, se presenta de forma sintética la contribución de estas prácticas.

Tabla 1
Identificación de la legislación aplicable (D1)

Pregunta	Práctica	¿De qué forma ocurre?
1.1	Esta cuestión comprueba cómo son los controles específicos y las responsabilidades individuales para cumplir con los requisitos reglamentarios, si se definen y documentan, permitiendo al usuario identificar diferencias y similitudes con las normas del ambiente interno y externo.	Control: procesos internos VSM; listas de verificación, conciliaciones, restricción de acceso al sistema SAP e indicadores de rendimiento; Responsabilidades individuales: conocimiento del funcionario; acceso a las transacciones del sistema. Documentación: carpeta en la red con acceso restringido a cada área.

Fuente: Datos de investigación.

Los gestores acreditan que esta práctica contribuye a la gobernanza corporativa en el requisito de conformidad. En este sentido, la coordinadora de contabilidad afirma: "*Los controles nos permiten garantizar que las informaciones fueron efectivas y son consistentes. Estos controles, [...] son necesarios para la elaboración de los estados financieros sin distorsiones [...] garantiza la conformidad de los estados financieros*".

La coordinadora fiscal también indica que: "*Si los controles no existiesen no se estaría seguro si el proceso es correcto [...]*". Alineada a esta percepción, la coordinadora de costos/planificación señala: *"[...] en mi visión, esos controles que hacemos hoy contribuyen a seguir la conformidad, en la propia validación de las informaciones*".

El gerente de control afirma: "*contribuye de forma vital [...] es muy importante que la gente tenga a las personas entrenadas, las personas en sus áreas de responsabilidad, con sus atribuciones bien definidas. [...] creo que eso facilita mucho la confiabilidad en la información [...]*". En la misma perspectiva el gerente financiero señala: "*estas normas definen un estándar y el estándar es muy importante [...]*". Bajo la óptica del área de TI, el supervisor de TI afirma:

"*garantiza que la información esté disponible cuando se solicita, tanto para el usuario interno como para el externo*". En la percepción del gerente de TI: *"[...] la regla tiene que ser seguida para mantener la conformidad, esa es la primera directriz [...]*".

Tabla 2
Derechos de propiedad intelectual (D2)

Pregunta	Práctica	¿De qué forma ocurre?
2.1	Esta cuestión verifica cómo ocurre la divulgación de la política de uso legal de productos *software* y de información. Debe exponerse de forma comprensible a los usuarios atendiendo a las normas reguladoras en el ambiente interno y externo.	Hay una política de uso legal de productos y software; es divulgada en el momento que el empleado ingresa en la empresa; el funcionario firma un término de responsabilidad; está disponible en la intranet; los gestores reciben por e-mail esta política; los gestores creen que esta política debería ser más difundida.
2.2	Esta cuestión comprueba si la adquisición de *software* se produce sólo a través de fuentes conocidas y de reputación para asegurar que los derechos de autor no están siendo violados y si esto ocurre de forma idéntica y uniforme previniendo el riesgo mediante la monitorización y supervisión de los procesos operativos.	La adquisición de *software* se produce solo por medio de fuentes conocidas y de reputación; hay un proceso de compra de *software* mediante tres ofertas que involucra a las áreas de compras, financiera y de TI; no hay evidencias de adquisición de *software* sin licencia; Los gerentes consideran que esta práctica mitiga los riesgos.
2.4	Esta cuestión comprueba cómo es el mantenimiento y la identificación de los registros de activos em cuanto a proteger los derechos de propiedad intelectual, si éstos ocurren sin omisión o distorsión, proporcionando evidencias a los *stakeholders*.	Hay restricción em la instalación de *software*; el mantenimiento y la identificación de los registros de activos ocurre solamente por medio de personas autorizadas de TI; hay protección y trazabilidad de los accesos indebidos por medio de informes internos generados por el sistema; los gestores consideran que está práctica no es evidenciada a los *stakeholders* al tratarse de un proceso interno.
2.5	Esta cuestión verifica si mantener pruebas y evidencias de propiedad evita la omisión o distorsión en las decisiones de los usuarios mediante la responsabilidad sobre las acciones propias o de los demás.	Los gestores consideran como prueba y evidencias: contraseña de acceso al sistema, usuario, firma del término de responsabilidad; estas pruebas y evidencias proporcionan trazabilidad, identificación y conocimiento de responsabilidades.
2.6	Esta cuestión tiene por objeto verificar si los controles neutralizan los sesgos y aseguran que el número de usuarios permitidos no excede el número de licencias adquiridas, cumpliendo las normas internas.	La empresa posee 200 licencias de acceso a SAP, el control de estas es realizado por el departamento de TI; se informa a la dirección los costos de estas licencias.
2.7	Esta cuestión identifica si las verificaciones de adquisición e instalación de *software* y licencias ocurren de la forma más completa posible, sin omisión de algún hecho relevante, permitiendo un clima de confianza.	Hay un seguimiento de TI principalmente en la fase inicial de la adquisición e instalación del *software* al proveedor y, posteriormente, la intervención de TI sólo ocurre cuando es necesario, ya que el proceso está estabilizado.
2.10	Esta cuestión verifica el cumplimiento de los términos y condiciones para el *software* y la información obtenidos a partir de redes públicas y, si esto puede ser verificable, previniendo el riesgo, realizando la monitorización y supervisión continua de los procesos.	Este cumplimiento se produce debido al bloqueo de determinados sitios; la restricción de acceso al usuario a internet, que sólo tiene acceso mediante la autorización de los gestores; internet se utiliza como herramienta de información; no hay acceso a las redes sociales; toda conexión pasa por un

		firewall que atiende a las políticas de seguridad de la empresa.
2.11	Esta cuestión aborda el no copiar en todo o en parte documentos en general, además de aquellos que están permitidos por la ley de derechos de autor. Este procedimiento evita las manipulaciones y debe considerar el comportamiento ético y moral.	Sólo los usuarios de sus respectivas áreas tienen acceso a las carpetas en la red y pueden copiar los documentos que están disponibles allí; se produce el bloqueo del acceso a las áreas no autorizadas; los USB de las máquinas están bloqueados para *pendrives.*

Fuente: Datos de investigación.

Se constató que todos los gestores creen que las prácticas evidenciadas en la Tabla 2 contribuyen. Según la coordinadora fiscal: "*Siguiendo estas reglas, comprar el software de fuentes conocidas mitiga el riesgo de divergencia y la pérdida de información, creo también que las limitaciones de acceso de determinados sitios pueden impedir la entrada de algunos virus [...] esto garantiza que la empresa está cumpliendo las normas [...]*".

En este sentido, la coordinadora contable afirma: *"[...] son prácticas que evitan pérdidas y retrasos en la entrega de las informaciones y nos garantiza resultados más seguros lo que contribuye a la conformidad*". El gerente financiero cree que *"[...] que la gente tenga una política de utilización del software de la empresa mitiga bastante el riesgo, saber lo que cada usuario está haciendo es muy importante. El momento que estamos nos permite saber que todo lo que es hecho por el usuario se tiene trazabilidad, no hay puntos oscuros, se tiene monitorizada la información [...]*".

Bajo la percepción del gerente de control las prácticas contribuyen porque *"limita el acceso, deja restringido a las personas en sus áreas de actuación [...] protege en relación a alguien que no tiene el conocimiento de trabajar con los documentos [...] Yo entiendo que eso trae una confianza en el proceso [...] ".* Esto es corroborado por la coordinadora de costos/planificación: *"Creo que la contribución es la limitación, la propia limitación de la información de cada sector [...] esas barreras contribuyen a la conformidad".*

Las respuestas obtenidas por los gestores de TI son similares a los demás gestores. El gerente de TI afirma: *"[...] creo que contribuyen a mitigar al máximo el riesgo, para que la gente mantenga la seguridad de la información*". El supervisor de TI complementa: "*Utilizamos todas estas prácticas para garantizar la seguridad de la información [...] y que nadie pueda manipular o perjudicar a la empresa [...]*".

Tabla 3
Protección de registros organizacionales (D3)

Pregunta	Práctica	¿De qué forma ocurre?
3.1	Esta cuestión comprueba si los registros almacenados tienen detalles de protección a lo largo del tiempo y están disponibles en un lugar adecuado.	Se almacenan en servidores. El servidor SAP se encuentra en un Datacenter ubicado en São Paulo; hay redundancia de generador, de energía eléctrica, de nobreak; hay otro servidor interno en el que se almacenan los archivos en *Excel*, red interna y documentos de la empresa; se realiza un proceso de copia de seguridad para la protección de los registros.
3.2	Esta cuestión comprueba cómo se almacenan las claves criptográficas o firmas digitales, así como si están libres de errores, sesgos y manipulaciones, ayudando a la prevención de riesgos, monitorización y supervisión continua de los procesos.	La firma digital se utiliza para la entrega de obligaciones en el ámbito fiscal y de control. El área financiera la utiliza para las transacciones bancarias; hay una contraseña y un token para enviar esa información; es necesaria la aprobación de dos procuradores de la transacción bancaria; la criptografía está en una fase inicial para los datos en portátiles; las firmas digitales están certificadas; todas las conexiones que llegan al servidor están encriptadas.
3.3	Esta cuestión verifica cómo son los cuidados en cuanto a la posibilidad de deterioro de los medios almacenados y, si esto ocurre de forma similar para ítems afines dentro de la estructura organizacional.	Se contacta con el equipo de medio ambiente para hacer el descarte adecuado con la empresa autorizada.
3.4	Esta cuestión verifica cómo son procedimientos para asegurar la capacidad de acceso a los datos contra pérdidas ocasionadas por futuros cambios en la tecnología, permitiendo a los usuarios identificar diferencias y semejanzas, interpretando y evaluando los reglamentos para limitar las pérdidas.	La empresa ha cambiado recientemente el sistema y los datos están disponibles en el sistema antiguo; la copia de seguridad garantiza el acceso a los datos. Este procedimiento limita las pérdidas y permite la comparabilidad, pues la información está disponible y accesible cuando se precisa.
3.5	Esta cuestión verifica cómo los datos pueden ser recuperados de forma aceptable, lo más completa posible y sin omisión, por medio de la monitorización y supervisión continua de los procesos.	La recuperación de los datos ocurre por medio de la copia de seguridad hecha diariamente para los movimientos de datos y, semanalmente se realiza la copia de seguridad completa de los datos; hay un gran volumen de datos y estos se graban en cinta; la monitorización ocurre vía *helpdesk* a través de las peticiones hechas por los empleados.
3.6	Esta cuestión verifica la destrucción de los registros, si no son necesarios para la organización, ocurre con cautela cumpliendo las normas reguladoras en el ámbito interno y externo.	Hay documentos físicos que son permanentes, por lo que no se pueden destruir. Para los archivos digitales hay copia de seguridad; el mantenimiento y el descarte son responsabilidad de cada área.
3.7	Esta cuestión verifica si la emisión de directrices generales para la retención, almacenamiento, tratamiento y disposición de los registros de información es capaz de predecir resultados futuros a través de normas reguladoras en el ámbito interno y externo.	La política de TI evidencia estas directrices: la información de SAP se encuentra en un Datacenter ubicado en São Paulo. Los archivos de red, accesos internos, documentos y archivos *Excel* se almacenan en un Datacenter ubicado a unos 500 metros de distancia de la empresa, en un edificio separado y dentro de una caja fuerte contra incendios; el acceso a él se limita a TI.
3.8	Esta cuestión verifica cómo es la planificación de la retención, la forma de identificar los registros esenciales y el período que cada uno debe ser mantenido	La custodia de los registros se produce en el sistema SAP en un Datacenter ubicado en São Paulo; se hace copia de seguridad de la información; los registros se producen por transacción y en varias tablas.

	de forma disponible y accesible a los usuarios.	
3.9	Esta cuestión comprueba cómo la información clave de los diferentes sistemas se mantiene / almacena y se transfiere a una base de datos de gestión.	La información se extrae del sistema SAP, no hay otro sistema para transferir la información clave; *Excel* y *Powerpoint* se utilizan sólo para algún formato de informe de gestión.

Fuente: Datos de investigación.

Los gestores creen que estas prácticas contribuyen a la conformidad. De acuerdo con el gerente de control: "*Creo que contribuyen, porque tenemos una única base que nos ayuda a tener la conformidad [...] tenemos backup del sistema, confiabilidad del sistema [...]*".

En la percepción de la coordinadora de costos/planificación esas prácticas "*ayudan al control [...] también a la confiabilidad que tiene el usuario a que la información está almacenada y que estará disponible cuando la necesite"*. Bajo la óptica del gerente financiero: "*Contribuyen sí. Pienso que esa cuestión de la seguridad de las firmas es muy importante [...]*".

La coordinadora fiscal afirma: *"Cada sector sólo tiene acceso a sus transacciones, entonces ahí se tiene una garantía de acceso a los datos permitidos, las personas tienen el conocimiento y entrenamiento para asignar los datos al sistema, cada área tiene su responsabilidad y eso con certeza contribuye"*. La coordinadora contable explica la importancia de estas prácticas y afirma que: *"Los registros contables son de gran importancia para la empresa, a través de ellos se produce la toma la decisión, deben ser confiables y claros, deben estar protegidos y archivados en lugares seguros, libres de riesgos, deben estar disponibles en cualquier momento [...]*.

Para el gerente de TI estas prácticas "*proporcionan la disponibilidad y la integridad de los datos, en el momento en que se hace una recuperación de algún dato [...]*". En este mismo sentido el supervisor de TI afirma: "*contribuyen justamente al conseguir hacer que la información esté disponible [...] siempre buscando la seguridad de la información y su disponibilidad*".

Tabla 4
Protección y privacidad de la información de identificación personal (D4)

Pregunta	Práctica	¿De qué forma ocurre?
4.1	Esta cuestión comprueba cómo es la política de privacidad y protección de datos de la	Hay un término de responsabilidad que trata sobre la confidencialidad de la información, que se firma

	organización, así como su relevancia permitiendo interpretar y evaluar los reglamentos para limitar las pérdidas.	en la contratación del funcionario; existe una política de privacidad y protección de datos.

Fuente: Datos de investigación.

Sólo los gestores de las áreas fiscal y de TI respondieron esta cuestión, los demás no supieron responder. La coordinadora fiscal afirma que: " *contribuye a que los funcionarios no puedan exponer a la empresa y evita rumores en el mercado*". El supervisor de TI añade la responsabilidad del empleado para lograr la conformidad y explica que: *"[...] en el momento en que el funcionario toma conciencia de su responsabilidad [...] va a reducir riesgos para la empresa*".

Tabla 5
Regulación de controles de criptografía (D5)

Pregunta	Práctica	¿De qué forma ocurre?
5.1	Esta cuestión verifica cómo es el uso de la encriptación, si ocurre con cautela de acuerdo con el cumplimiento de normas reguladoras internas.	El usuario, la contraseña compleja según las normas internas, la encriptación de la información que garantiza la seguridad de la información.
5.2	Esta cuestión verifica cómo la asesoría jurídica garantiza la conformidad con la legislación y las regulaciones, de forma que posibilita que la información está libre de errores, sesgos y manipulaciones, por medio del cumplimiento de normas internas y externas.	Toda modificación, inclusión y exclusión de un contrato pasa por la asesoría jurídica. Algunos ejemplos: contratos de alquileres, contratos de clientes y proveedores, transacciones entre las empresas, contratación de consultoría, elaboración de términos de responsabilidad; el conocimiento de la legislación; el aval de un especialista en el área mitiga los riesgos.

Fuente: Datos de investigación.

En cuanto a la contribución de estas prácticas para la conformidad, se constató que la práctica de criptografía fue evidenciada apenas por el área de TI. Según el supervisor de TI: "*con la criptografía la empresa ofrece seguridad para el uso a sus colaboradores sea un software, internet o cualquier otra cosa [...] la gobernanza trabaja en este sentido, de que las informaciones estarán disponibles y seguras*". Sin embargo, el gerente de TI afirma que la contribución puede ser mejorada: "*Puede contribuir a hacer efectivo el uso de la criptografía, colocar la criptografía internamente en los datos críticos [...]*".

En lo que se refiere a la asesoría jurídica todos los gestores acreditan que contribuye a la conformidad. Según la coordinadora de contabilidad: "*Las asesorías jurídicas garantizan que la información sea de conformidad con la legislación*". La coordinadora fiscal afirma que: "*[...] hay un conocimiento más específico del área tributaria, contribuye de forma preventiva minimizando los riesgos*". La coordinadora de costos/planificación complementa

señalando: "*[...] contribuye porque nos da seguridad [...] tenemos un respaldo de personas específicas sobre el asunto*".

En este sentido, el gerente financiero indica que la asesoría jurídica es esencial, afirma que: "*La cuestión jurídica contribuye, pues se tiene el fundamento técnico y legal de que aquellos contratos que están siendo firmados están amparados judicialmente, para evitar poner en riesgo la salud de la compañía. Creo que es esencial el paso por el área jurídica*". Esto es corroborado por el gerente de control: "*la cuestión jurídica es importante porque no somos expertos en esta área*".

Bajo la perspectiva de la gerente de TI, la asesoría jurídica contribuye "*[...] con las acciones de acompañamiento contractual o seguimiento de acciones irregulares internas de los usuarios, en este sentido nos apoyan para que la gente tenga siempre la conformidad de los procesos y mantener la seguridad de la información*".

Tabla 6
Análisis crítico independiente de la seguridad de la información (D6)

Pregunta	Práctica	¿De qué forma ocurre?
6.1	Esta cuestión verifica cómo se ejecuta el análisis crítico y, si éste refleja lo que ocurrió independientemente de un contrato. Debe proporcionar evidencia a los *stakeholders* sobre la atención de una expectativa o el cumpliendo con su deber.	La auditoría crítica es realizada por una auditoría externa; KPMG realiza trimestralmente la auditoría contable, financiera y de procesos; proporciona evidencia a los *stakeholders* a través de los dictámenes de auditoría; proporciona información a través de un informe que está a disposición de los gestores y de la dirección.
6.2	Esta cuestión comprueba cómo los resultados del análisis crítico independiente se registran y se comunican a la dirección. Esto ocurre de forma neutra, no habiendo resultado a través de informaciones útiles a los usuarios, permitiendo un clima de confianza.	Los resultados se reportan a la dirección a través de un informe trimestral, un dictamen de auditoría. Internamente existe un *software* para evidenciar las consideraciones de la auditoría externa (*Teammate*), así como presentar el plan de acción de los gestores; se trata de un órgano independiente que tiene responsabilidades en cuanto a la validación de los estados financieros de la empresa.

Fuente: Datos de investigación.

Los gestores señalan la contribución de estas prácticas a la conformidad. De acuerdo con la coordinadora fiscal "*[...] cumplir la legislación y tener una revisión de una auditoría independiente asegura que no hay ocultación y contribuye a reducir los riesgos*". La coordinadora contable explica también la contribución de estas prácticas: "*El análisis crítico de los registros, informes, procesos y de los estados financieros es de gran importancia para la validación de las informaciones generadas por la contabilidad [...]*".

En este sentido el gerente financiero afirma que la visión de una empresa independiente contribuye a la mejora de los procesos y a su conformidad. Él explica que: *"[...] cuando la gente está involucrada en los procesos muchas veces no ven los fallos [...] puede no tener una visión imparcial [...] Creo que contribuye mucho tener una mirada de una auditoría independiente [...] Ayuda mucho a la gente a mejorar los procesos a través de sugerencias de mejora, si tienen una retroalimentación".*

La gran contribución según la percepción de la coordinadora de costos/planificación es la que garantiza la auditoría externa. Según esta gestora*: "La práctica más fuerte que tenemos es la auditoría externa por ser una empresa de capital abierto que tenemos que seguir leyes de CVM, de IFRS [...] Esta es la mayor garantía que tiene la gente, cuando la auditoría externa da el aval, ellos se comprometen también con la información divulgada [...] el cumplimiento de las obligaciones legales ayuda a la conformidad ".*

Según la gerente de TI: "*Estas prácticas contribuyen sí, principalmente a la reducción del riesgo, pues la auditoría externa valida las informaciones y también chequea los procesos internos*". El supervisor de TI complementa indicando que: "*el área de TI es un área que cambia mucho y si no está detrás de las nuevas tecnologías de seguridad esto puede llevar a vulnerabilidades, por lo que creo que contribuye*".

Para el gerente de control: "*contribuye mucho a garantizar la conformidad y a mitigar los riesgos [...] si se tiene el proceso interno y luego un proceso de validación por parte de la auditoría externa, entiendo que eso da la seguridad a los clientes externos, stakeholders y accionistas, para que confíen en los números de la compañía [...]*".

Tabla 7
Conformidad con las políticas y procedimientos de seguridad de la información (D7)

Pregunta	Práctica	¿De qué forma ocurre?
7.1	Esta cuestión verifica cómo los gestores implementan acciones correctivas tras la detección de la no conformidad. Si esto ocurre de la forma más completa posible, sin omisión de algún hecho relevante, actuando con responsabilidad por las acciones propias o de los demás.	Se verificó que los gestores establecen las acciones correctivas después de la detección de no conformidades por medio de manuales, dibujos del proceso, solicitudes a TI y conversaciones con los empleados.
7.2	Esta cuestión verifica si los resultados de los análisis críticos y de las acciones correctivas determinadas por los gestores son registrados y mantenidos mediante informaciones íntegras y oportunas de acuerdo con las normas reguladoras internas y externas.	El registro se produce en carpetas ubicadas en la red de cada área específica; en los manuales de procesos (VSM); en el sistema SAP; también hay una copia de seguridad de esta información.

Fuente: Datos de investigación.

En cuanto a la contribución de las prácticas evidenciadas en la Tabla 7, el gerente financiero afirma que: *"[...] contribuyen en la medida en que toda la información divulgada al mercado está alineada, no sólo con las normas contables, sino con las normas de cumplimiento también [...] La propia cuestión de que la empresa esté en el nivel 2 de la gobernanza corporativa ya posibilita esa integridad".*

La coordinadora de contabilidad también señala: "*La importancia de la seguridad de las contraseñas de acceso es responsabilidad de los usuarios y debe cumplirse para garantizar la seguridad de las informaciones [...]*". Esta percepción es corroborada por el gerente de TI: "*El cumplimiento de estas prácticas y la mejora de ellas también contribuye, a mitigar el riesgo de seguridad*". El supervisor de TI complementa: "*[...] Creo que estas prácticas sólo benefician a la empresa [...]*".

La coordinadora de costos/planificación también explica: "*[...] que tener la seguridad de la auditoría independiente, en el sentido de apuntar o no algún fallo, que son el vínculo de confianza con el equipo de trabajo [...]*". Según la coordinadora fiscal: "*[...] de esta forma la gente evita exponer a la empresa, causar algún riesgo de imagen y también financiero*". Bajo la óptica del gerente de control estas prácticas "*contribuyen porque traen mejoras al proceso [...] contribuyen al garantizar la exactitud de la información, al garantizar que los procesos efectivamente ocurran interna y externamente, pues se tiene el proceso de auditoría validando todo ello*".

Tabla 8
Análisis crítico de la conformidad técnica (D8)

Pregunta	Práctica	¿De qué forma ocurre?
8.1	Esta cuestión identifica cómo se producen las pruebas de intrusión o la evaluación de vulnerabilidades y si se planifican, se documentan y reproducen cuando hay incertidumbres. Para prevenir riesgos, monitoreando y supervisando continuamente los procesos operativos.	La empresa utiliza un firewall que bloquea las entradas indebidas y posibles intrusiones para limitar el acceso y reducir las vulnerabilidades; el control se realiza diariamente por el área de TI, a través del informe de los intentos de acceso.
8.2	Esta cuestión identifica si la verificación de conformidad técnica solo es ejecutada por personas autorizadas y competentes, o bajo la supervisión de dichas personas. Con el fin de proporcionar evidencia a los *stakeholders* sobre la atención de una expectativa.	La verificación de conformidad técnica ocurre solamente por personas capacitadas. Se produce por analistas, especialistas, supervisores y gerentes.

Fuente: Datos de investigación.

Los gestores consideran que las prácticas evidenciadas en la Tabla 8 contribuyen a la gobernanza corporativa en el requisito de conformidad. La coordinadora contable afirma: "*Una buena herramienta de gestión contribuye a la toma de decisiones, auxilia en la gestión de la empresa con informaciones integrales, seguras y en tiempo real. La calidad de la información también está garantizada con profesionales cualificados en la estructura funcional de la empresa [...]*".

Bajo la óptica de la coordinadora fiscal: "*El control de invasión asegura que no entra en la empresa cualquier información, el bloqueo de determinados sitios. Las personas cualificadas y entrenadas minimizan el riesgo de emplear una información errónea*".

En relación a ello, el gerente de control afirma: "*Contribuye a tener especialistas tratando [...] que garantizan un nivel de precisión muy bueno, [...] contribuye en el momento que se limitan las vulnerabilidades en el sentido de no tener sistemas paralelos, con cambios de interfaz, hoy todo eso está centralizado dentro del sistema [...]*".

Alineado con a estas percepciones, el gerente de TI explica: "*Creo que contribuyen. La gente mantiene la seguridad de la información en función de los accesos, de la confianza en el firewall. Estas prácticas ayudan a mitigar el riesgo de seguridad*". El supervisor de TI complementa afirmando que estas prácticas "*mantienen la integridad y la seguridad de la información*". La coordinadora de costos/planificación considera que estas prácticas deben mejorarse. Según esta gestora: "*[...] Estas prácticas tienen que ser más aplicadas en el sentido de que el sistema ayude a la interpretación*". Esto también es percibido por el gerente financiero: *"[...] creo que va mucho sobre la percepción de la contabilidad para garantizar que la información esté de acuerdo con los estándares contables actuales [...]*".

4.3 Contribución a la conformidad

En base a las entrevistas realizadas, se destacan las siguientes palabras clave: información, acceso, conformidad, proceso, mejora de proceso, control, cumplimiento, legislación, auditoría independiente, confianza, disponibilidad, integridad, responsabilidad, validación, seguridad de la información, mitigar los riesgos.

Los gestores destacan la "información" en todos los dominios de la investigación, tanto en lo que se refiere a informaciones internas como externas. Se destacó como el activo más valioso que tiene la empresa, por lo tanto, está alineado con Ribeiro Filho, Lopes y Perdeneiras (2009) así como con el abordaje de Sêmola (2014). La "información" fue vinculada con diversas

características cualitativas, como: accesibilidad, conformidad, confianza, disponibilidad, integridad, seguridad de la información, validación y responsabilidad.

El "acceso" citado por los gestores está presente en los ámbitos: D2; D3; D7 y D8. Se refiere al acceso a la información y también a las limitaciones de acceso. Los accesos internos y externos posibilitan la toma de decisiones y abordan el concepto de accesibilidad evidenciado por Ferreira et al. (2015); Gerard y Weber (2015); Mateescu (2015); Oliveira et al. (2015). En cuanto a las limitaciones de acceso, sólo tienen permiso de acceso a las transacciones y carpetas de red los usuarios con el perfil autorizado por el gestor. Este procedimiento según los gestores protege la información contra accesos no autorizados. Estas limitaciones convergen con las recomendaciones de la norma ISO/IEC 27002:2013 y con los trabajos de Albertin y Pinochet (2010) y Sêmola (2014).

La "conformidad" es destacada por todos los gestores y está presente en todos los ámbitos, excepto en el dominio D4, fue evidenciada con el fin de cumplir los requisitos internos y externos de la organización. Los controles, las responsabilidades individuales, las mejoras de proceso, las políticas internas, el cumplimiento de la legislación y la auditoría independiente son requisitos fundamentales para la conformidad. El concepto de conformidad abordado por los gestores converge con Ferreira et al. (2015); Mateescu (2015) y Griffith et al. (2016). La percepción de los gestores está alineada también con el estudio de Turrent y Ariza (2016) el cual indica que la conformidad de la gobernanza corporativa propicia un mayor control y mantenimiento de la reputación en el mercado. En esta investigación se ha constatado que los controles y procesos estandarizados y sistematizados contribuyen a la conformidad de las informaciones.

Otro concepto destacado por los gestores se refiere a la “confianza”, que está presente en todos los dominios, excepto en los dominios D4 y D5. La confianza de la información está ligada al entrenamiento de los usuarios, sus responsabilidades, las atribuciones, la protección de los registros organizacionales y al diseño de los procesos internos. La auditoría externa contribuye también a la confiabilidad de la información, pues valida la información dando confianza a los *stakeholders*. En este sentido, la "confiabilidad" evidenciada por los gestores significa que el usuario acepta la información y la utiliza como base para la toma de decisiones (Hendriksen & Van Breda, 1999; Ribeiro Filho, Lopes & Perdeneiras, 2009; Iudícibus (2010); CPC 00 R1 (2011); Souza et al. (2015); Jorissen (2015); Azad et al. (2016), así como que la actuación del sistema ocurre como se esperaba (Albertin & Pinochet, 2010).

La palabra "disponible" remite a la palabra "disponibilidad" y fue evidenciada por los gestores en los ámbitos: D1; D3 y D5. Los gestores señalan que el sistema proporciona la información a los usuarios internos y externos, así como el *backup* de los datos permite su disponibilidad de forma completa e íntegra. El cifrado también fue destacado en el sentido de hacer disponible la información segura. Las indicaciones de los gestores están alineadas con Hendriksen y Van Breda (1999), Dhillon y Backhouse (2000); Ribeiro Filho; Lopes y Perdeneiras (2009); Iudícibus (2010); Albertin y Pinochet (2010); CPC 00 R1 (2011); Souza et al. (2015); Safa et al. (2015); Jorissen (2015) y Azad et al. (2016).

El concepto "integridad" también fue abordado por los gestores y está presente en los dominios: D2; D3; D7 y D8. Las prácticas evidenciadas en estos ámbitos abordan la integridad como la garantía de que nadie pueda manipular la información o perjudicar a la empresa. Los registros contables, la recuperación de datos (*backup/restore*), divulgación de los datos, validación por la auditoría externa, nivel 2 de la gobernanza corporativa, sistema integrado, profesionales cualificados y limitaciones de acceso, son ejemplos citados por los gestores. La integridad converge con la protección contra alteraciones indebidas (Dhillon & Backhouse, 2000; Albertin & Pinochet, 2010; Sêmola, 2014; Uddin & Preston, 2015; Safa et al., 2015), así como con la información más completa posible sin omisión de algún hecho relevante (Hendriksen & Van Breda, 1999; Ribeiro Filho, Lopes & Perdeneiras, 2009; Iudicibus, 2010; CPC 00 R1 (2011); Souza et al., 2015; Jorissen, 2015; Azad et al., 2016.

En cuanto a la "responsabilidad" fue evidenciada por los gestores en los ámbitos: D1; D3; D4 y D7. Se refiere a la responsabilidad del funcionario, el área de actuación, la auditoría externa, las firmas digitales y la autorización para transacciones. Se entiende que la responsabilidad significa responder por las acciones propias o de los demás (Ferreira et al., 2015; Gerard & Weber, 2015; Mateescu, 2015; Oliveira et al., 2015).

El concepto "validación" fue abordado por los gestores en los ámbitos: D1; D6 y D7. Los gestores afirman que la validación de la información ocurre por medio de análisis críticos internos dentro del sector de actuación del gestor. La validación externa ocurre por un órgano independiente, siendo éste destacado constantemente por los gestores. La validación remite al concepto de "autenticidad" y está alineada con Sêmola (2014).

La "seguridad de la información" se ha comunicado en los ámbitos: D2; D3; D5; D7 y D8. Los gestores señalan que las prácticas evidenciadas en estos ámbitos contribuyen a la conformidad. Se relacionó la seguridad de la información con los conceptos de integridad, disponibilidad, políticas de seguridad, conformidad, confiabilidad, confidencialidad y

autenticidad. Esto converge con Dhillon y Backhouse (2000); Albertin y Pinochet (2010); Bulgurcu, Cavusoglu y Benbasat (2010); Fontes (2012); Sêmola (2014); Uddin y Preston (2015); Safa et al. (2015). Sin embargo, los gestores atribuyeron también a la seguridad de la información los conceptos de responsabilidad y accesibilidad.

En cuanto a "mitigar los riesgos", el término fue referido por los gestores en todos los dominios excepto en el dominio D1. Algunos ejemplos citados por los gestores se refieren a: licencias, políticas de utilización de *software*, trazabilidad de la información, integridad de la información, base única de datos, *backup*, confianza en el sistema, término de responsabilidad firmado por el funcionario, asesoría jurídica, auditoría externa en la validación de la información y verificación de los procesos internos, y procesos diseñados. Estas normas y procedimientos también mitigan el riesgo de divergencia y pérdida de información. Los ejemplos citados por los gestores están alineados con el concepto de evaluación de riesgos de Griffith et al., (2016).

En base al análisis cualitativo de las entrevistas realizadas se observó que las prácticas de seguridad de la información evidenciadas en la ISO/IEC 27002:2013, integradas en los conceptos de calidad de la información contable, contribuyen a la conformidad de la gobernanza corporativa.

5 Consideraciones finales

En esta investigación se ha analizado cómo las prácticas de seguridad de la información contable pueden contribuir a la Gobernanza Corporativa en el requisito de conformidad. Este objetivo fue alcanzado a partir de entrevistas con los gestores de las áreas de contabilidad, fiscal, costos/planificación, control, finanzas y TI, y se confirmó por medio del análisis documental.

Se verificó que la empresa posee política de seguridad de la información; política de tecnología de la información; política corporativa de seguridad de SAP; manual de conducta sobre uso, divulgación y mantenimiento de secreto sobre la información; y código de conducta; asimismo la empresa no tuvo ninguna reserva en los informes de auditores independientes sobre los estados financieros ni en la información trimestral en el período 2014 - 2016.

Se concluye que de las 41 prácticas de seguridad de la información contable (Fontana, 2017) la empresa utiliza 27. La investigación proporciona evidencias a los gestores y directivos y a los usuarios de la información, sobre cómo las prácticas de seguridad de la información contable pueden contribuir a la gobernanza corporativa en el requisito de conformidad. Se constató que

los controles; procesos internos VSM; listas de comprobación; conciliaciones; restricción de acceso al sistema, internet y carpetas en la red; indicadores de desempeño; responsabilidad individual; política de uso legal de productos y *software*; termino de responsabilidad; adquisición de *software* sólo por fuentes conocidas; restricción de instalación de *software*; *firewall*; políticas de seguridad; servidores en un lugar adecuado; firma digital; cifrado; *backup* de los datos; única base de datos; asesoría jurídica y auditoría externa, contribuyen proporcionando accesibilidad, conformidad, confiabilidad, disponibilidad, integridad, responsabilidad, autenticidad y seguridad de la información, y mitigan los riesgos de la organización.

Esta investigación contribuye en el ámbito académico mediante la creación de un modelo teórico generado a partir de la revisión de la literatura. Asimismo, contribuye en el ámbito profesional al profundizar en el fenómeno estudiado pudiendo ser transferible a otros contextos.

Se recomienda la realización de investigaciones involucrando estudios de casos múltiples, pues pueden contribuir a la identificación de nuevos elementos, así como realizar estudios que consideren empresas de otros sectores.

Por último, se recomienda llevar a cabo estudios que involucren otros principios de la gobernanza corporativa, como la transparencia, equidad, rendición de cuentas o responsabilidad corporativa, para identificar cómo las prácticas de seguridad de la información pueden contribuir a estos principios.

Referencias

Adiloglu, B., & Vuran, B. (2012). The relationship between the financial ratios and transparency levels of financial information disclosures within the scope of corporate governance: Evidence from Turkey. *Journal of Applied Business Research*, *28*(4), 543-554.

Albertin, A., & Pinochet, L. (2010). *Política de segurança de informações: uma visão organizacional para a sua formulação*. São Paulo: Elsevier.

Azad, R., Azad, R., Azad, K., & Akbari, F. (2016). The effect of cost accounting system inventory on increasing the profitability of products. *Journal of Industrial and Intelligent Information*, *4*(1), 83-87.

Barbosa, J., Scherer, L., Scarpin, J. E., & Murcia, F. (2015). Construction of a metric of quality of accouting information from the perspective of fundamental analysts. *Revista de Contabilidade e Organizações*, *9*(24), 42-55.

Buccafurri, F., Fotia, L., Furfaro, A., Garro, A., Giacalone, M., & Tundis, A. (2015). An analytical processing approach to supporting cyber security compliance assessment. *Proceedings of the 8th International Conference on Security of Information and Networks*, 46-53.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

Collis, J., & Hussey, R. (2005). *Pesquisa em administração: um guia prático para alunos de graduação e pós-graduação* (2ª ed.). Porto Alegre: Bookman.

CPC 00 R1 (2011). *Estrutura conceitual para elaboração e divulgação de relatório contábil-financeiro*. Comitê de Pronunciamentos Contábeis. Disponible en: https://bit.ly/2x9wlvM. Consulta: 28 octubre 2018.

Darounco, J. M. (2013). *Análise de processo de controles internos e de TI no requisito de conformidade da governança corporativa*. Dissertação Mestrado em Ciências Contábeis, Universidade do Vale do Rio dos Sinos.

Dedonatto, O., & Beuren, I. M. (2010). Análise dos impactos para a Contabilidade no processo de implantação da governança corporativa em uma empresa. *Revista Contabilidade e Controladoria*, *2*(3), 23-38.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Ferreira, E., Matos, F., Matos, D., Bugarim, M. C., & Machado, D. (2015). Governança corporativa na saúde suplementar: Estudo de caso em uma operadora de plano de saúde. Pensamento & Realidade. *Revista do Programa de Estudos Pós-Graduados em Administração-FEA*, *29*(3), 19-39.

Fontana, K. (2017). *Análise das práticas de segurança da informação contábil e sua contribuição para a governança corporativa no requisito de conformidade*. Dissertação Mestrado em Ciências Contábeis, Universidade do Vale do Rio dos Sinos.

Fontes, E. (2012). *Políticas e normas para a segurança da informação: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações* (1ª ed.). Rio de Janeiro: Brasport.

Gerard, J. A., & Weber, C. M. (2015). Compliance and corporate governance: theoretical analysis of the effectiveness of compliance based on locus of functional responsibility. *International Journal of Global Business*, *8*(1), 15-26.

Griffith, S. J., Thel, S., Baer, M., Miller, G. P., Manwah, G., Breslow, S., Cohen, A., Grant, M., Klehm, H., Meyer, A., & Baxter Jr, T. C. (2016). The changing face of corporate compliance and corporate governance. *Fordham Journal of Corporate & Financial Law*, *21*(1), 1- 71.

Hendriksen, E., & Van Breda, M. (1999). *Teoria da contabilidade* (5ª ed.). São Paulo: Atlas.

IBGC (2009). *Código das melhores práticas de governança corporativa* (4ª ed.). São Paulo: Instituto Brasileiro de Governança Corporativa. Disponible en: https://bit.ly/2Q0SUKi. Consulta: 28 octubre 2018.

ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls*. International Organization for Standardization (ISO).

Iudícibus, S. (2009). *Teoria da contabilidade* (9ª ed.). São Paulo: Atlas.

Iudícibus, S. (2010). *Manual de contabilidade e societária: Aplicável a todas as sociedades de acordo com as normas internacionais e do CPC* (1ª ed.). São Paulo: Atlas.

Jorissen, A. (2015). The IASB: From high quality accounting information towards information to foster trust and stability in global markets. *Revista Contabilidade & Finanças, 26*(69), 243-246.

Lima, A. S., Carvalho, E. V., Paulo, E., Girão, L. F. (2015). Estágios do ciclo de vida e qualidade das informações contábeis no Brasil. *Revista de Administração Contemporânea*, *19*(3), 398-418.

Mateescu, R. A. (2015). Corporate governance disclosure practices and their determinant factors in European emerging countries. *Journal of Accounting and Management Information Systems*, *14*(1), 170-192.

Oliveira, D., Silva, M. P., Lima, T. A., & Souza, M. M. (2015). Um estudo exploratório da gestão de pessoas na integração e disseminação da governança corporativa. *Revista Acadêmica Augusto Guzzo*, *2*(16), 241-268.

Parsons, K. M., Young, E., Butavicius, M. A., Mccormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117-129.

Ribeiro Filho, J. F., Lopes, J., & Pederneiras, M. (2009). *Estudando teoria da contabilidade* (1ª ed.). São Paulo: Atlas.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Sêmola, M. (2014). Gestão da segurança da informação: Uma visão executiva (2ª ed.). Rio de Janeiro: Elsevier.

Shamala, P., Ahmad, R., Zolait, A. H., & Sahib, S. (2015). Collective information structure model for Information Security Risk Assessment (ISRA). *Journal of Systems and Information Technology*, *17*(2), 193-219.

Souza, P., Kopack, J., Borgert, A., Flach, L., & Lunkes, R. (2015). Estudo sobre o uso dos atributos da contabilidade gerencial em empresas de capital aberto do setor de energia elétrica. *Revista Ambiente Contábil-Universidade Federal do Rio Grande do Norte*, *7*(2), 215-230.

Turrent, G., & Ariza, L. (2016). Corporate governance ratings on listed companies: An institutional perspective in Latin America. *European Journal of Management and Business Economics*, *25*(2), 63-75.

Uddin, M., & Preston, D. (2015). Systematic review of identity access management in information security. *Journal of Advances in Computer Networks*, *3*(2), 150-156.

Yousuf, S., & Islam, Md. A. (2015). The concept of corporate governance and its evolution in Asia. *Research Journal of Finance and Accounting*, *6*(5), 19-25.