"Fortalecimiento del Sistema de control interno en la Entidad Educativa IFB con base en la metodología COSO-2013"

Trabajo de Investigación presentado para optar al

Grado Académico de Magíster en Auditoría

Presentada por:

Sr. John Erick Espinola Arteaga

Sra. Guadalupe Urbina Lozada

Asesor: Profesor José Díaz Ismodes

2015

Dedicamos el presente trabajo de investigación a nuestros padres, a nuestros compañeros de vida, y nuestros amigos más cercanos por su incondicional apoyo y confianza. Agradecemos a nuestros compañeros de trabajo, quienes en el día a día permitieron reforzar nuestros conocimientos a fin de contar con las herramientas necesarias para poder afrontar el desafío de desarrollar el presente trabajo, agradecemos también y de manera muy especial a nuestros profesores de la maestría quienes influyeron con sus lecciones de vida y experiencias profesionales y propiciaron el cumplimiento de nuestro objetivo, el cual vemos reflejado en el desarrollo del presente trabajo.

Resumen Ejecutivo

El presente trabajo de investigación se desarrolla en el Instituto de Educación Superior Tecnológico Privado de Formación Bancaria – IFB Certus, que es una organización educativa sin fines de lucro, enfocada en el crecimiento y desarrollo del alumnado, ofreciendo 4 carreras técnicas: Administración Bancaria, Contabilidad, Negocios Internacionales y Administración de Negocios y Gestión del Emprendimiento.

La necesidad principal de IFB Certus es fortalecer su sistema de control interno debido al rápido crecimiento que viene experimentando en los últimos años por el incremento de la demanda educativa en el país. Este crecimiento genera que la Entidad se encuentre en un proceso de expansión a nivel nacional y de mejora de sus procesos para la atención tanto del cliente externo como del interno. Estas actividades demandan una importante inversión en recursos financieros y en capital humano, generando constantes cambios en el entorno en el que se desarrolla (económico, social y normativo, entre otros)

El objetivo principal de este trabajo de investigación es proponer los lineamientos para la adecuación del Sistema de Control Interno sobre la base del marco COSO 2013 en IFB Certus.

Para lograr lo descrito en el párrafo anterior, se realizó el diagnóstico de la situación actual de la Entidad sobre la base del Marco COSO 2013. Al determinar el grado de madurez del control interno, se procedió a diseñar y proponer planes de acción que permitan superar las brechas en relación con un Sistema de Control Interno fortalecido. Asimismo, se elaboró una "Hoja de Ruta" para la revisión y priorización de oportunidades de mejora, considerando el grado de complejidad de la implementación, el impacto en el sistema de control interno, el tiempo y el costo de su ejecución.

La implementación de cada plan de acción nos indica que el fortalecimiento se irá dando progresivamente a corto, mediano y largo plazo; esto, siempre y cuando la Alta Dirección disponga de recursos suficientes para el desarrollo del proyecto y, a su vez, transmita a la Organización, en todos los niveles, la importancia del control interno para alcanzar los objetivos, incrementar los niveles de competitividad por medio de una administración transparente y así aumentar la rentabilidad.

Índice

Índice de tablas

Índice de gráficos

Índice de anexos

Capítulo I. Definición del problema

1. Problema

La Entidad Educativa IFB durante el proceso de expansión a nivel nacional y en la mejora de sus procesos tanto para la atención del cliente externo como del interno ha identificado deficiencias en el control interno, generando pérdidas económicas importantes y, a su vez, se incrementa la posibilidad de que la Entidad no alcance los objetivos estratégicos planteados por la Alta Dirección que ha definido 4 criterios: crecimiento, rentabilidad, calidad y posicionamiento, con la finalidad de crear, conservar y materializar el valor para sus grupos de interés.

Debido al incremento de la demanda académica en el país en los últimos años, la Entidad ha experimentado un considerable crecimiento en el número de alumnos. Esto ha determinado que los procesos actuales no se encuentren diseñados para soportar el constante crecimiento en especial en el control interno cuya finalidad es salvaguardar los activos de esta, enfocando sus esfuerzos a mitigar las eventualidades con impacto negativo en el desarrollo de sus actividades. De no ser atendidas estas, generarán pérdidas económicas y daños a la imagen institucional, entre otros. Asimismo, los colaboradores no se encuentra familiarizados de forma adecuada con buenas prácticas de control interno dando paso a la improvisación, toma de decisiones no alineadas con los objetivos de la Entidad y un inadecuado uso de los recursos de carácter económico, humano y material.

La preocupación constante de la Entidad es de contar con un adecuado Sistema de Control Interno que permita sostener el crecimiento constante de las operaciones, dar una seguridad razonable a los grupos de interés sobre la óptima administración de los recursos, y permitir que los esfuerzos de la Alta Dirección y sus colaboradores se encuentren principalmente enfocados a alcanzar los objetivos estratégicos planteados.

En la actualidad, la Entidad Educativa IFB tiene diversos problemas, a los que debe hacer frente para alcanzar sus objetivos, siendo una de sus principales preocupaciones el fortalecer el Sistema de Control Interno en todos los niveles de la organización y que, a su vez, contribuya en la mejora de sus procesos. Unos de los principales retos que tendrá la Alta Dirección para alcanzar los objetivos estratégicos será el implementar un adecuado Sistema de Control Interno para lo que se precisa obtener un diagnóstico de su situación actual con una metodología estándar que identifique brechas y oportunidades de mejora; así como un plan de implementación de las oportunidades de mejoras detectadas.

2. Objetivos de la investigación

2.1 Objetivo general

Proponer los lineamientos para la adecuación del Sistema de Control Interno sobre la base del Marco COSO 2013 en la Entidad Educativa IFB

2.2 Objetivos específicos

- Diagnosticar el nivel de madurez del Sistema de Control Interno de la Entidad, utilizando como referencia el nuevo marco COSO (2013).
- Diseñar y proponer planes de acción para el fortalecimiento del Sistema de Control Interno en referencia a las brechas identificadas en el diagnóstico realizado.
- Diseñar y proponer la "Hoja de Ruta" para la implementación de los planes de acción, respetando la priorización acordada con la Alta Gerencia de la Entidad y la situación deseada a mediano y largo plazo.
- Evaluar la viabilidad de los planes de acción para el logro de la situación deseada.

3. Alcance

Sobre la base de los cinco (05) componentes del control interno y los diecisiete (17) principios asociados a los componentes establecidos por el Marco Integrado de Control Interno publicado por el *Committe of Sponsoring Organizations of the Treadway Commission* (COSO) en el año 2013, se definirán y propondrán los lineamientos para la adecuación del Sistema de Control Interno de la Entidad Educativa IFB.

4. Limitaciones

Durante la elaboración del presente trabajo de investigación identificamos las siguientes limitaciones:

- La información de carácter confidencial como sueldos y plan estratégico, que fue proporcionada durante la investigación, no puede ser plasmada literalmente en el presente trabajo a solicitud explícita de la Entidad.
- La cantidad máxima de hojas y el tamaño permitido para los anexos en el presente trabajo de investigación no permiten transmitir íntegramente al lector la información recabada por la "herramienta para la evaluación de la situación actual del Sistema de Control Interno sobre la base del marco COSO 2013", que describe adecuadamente cada componente del Sistema de Control de la Entidad evaluada.

5. Pregunta de investigación

Por lo expuesto en los puntos anteriores, los integrantes del grupo nos planteamos la siguiente interrogante:

¿Cómo la Alta Dirección de la Entidad Educativa IFB puede mejorar su Sistema de Control Interno para incrementar las posibilidades de alcanzar los objetivos estratégicos definidos por la organización?

Capítulo II. Introducción

En los últimos años, el Perú goza de un crecimiento económico; por tal motivo, las empresas requieren trabajadores con determinadas capacidades y niveles de capacitación. Esto exige que la oferta de formación busque satisfacer la demanda de los potenciales estudiantes, que se ha incrementado a pasos agigantados en las últimas décadas.

El Instituto de Formación Bancaria - IFB CERTUS, en adelante la "Entidad", es una organización educativa sin fines de lucro, con 20 años de experiencia, enfocada al crecimiento y desarrollo del alumnado, con profesores especialistas en cada una de las cuatro carreras que ofrecen que son: Administración Bancaria, Contabilidad, Negocios Internacionales y Administración de Negocios y Gestión del Emprendimiento. La creación de la Entidad se da principalmente por una escasa oferta en capacitación en el sector financiero, lo cual generaba costos altos de especialización y productos de baja calidad; y también, un bajo nivel de bancarización en el país creando una brecha culturar/técnica creciente entre las Pymes y la Banca.

La Entidad es reconocida para otorgar títulos profesionales a nombre de la Nación siendo supervisada por el Ministerio de Educación. Tiene como público objetivo los jóvenes que han culminado sus estudios secundarios, principalmente de los sectores socio económicos C, D y E.

En 1995, la Asociación de Bancos del Perú (ASBANC) constituyó el Instituto de Formación Bancaria con la misión de elevar la especialización y cultura financiera en el país con excelencia educativa, formando recursos humanos calificados para el sector bancario, financiero y empresarial. Además, como responsabilidad social con la comunidad, se desarrollaron herramientas para la inclusión bancaria y financiera a través de programas gratuitos de capacitación a microempresarios, jóvenes y maestros de escuelas públicas a nivel nacional, ofreciendo competencias para mejorar la inserción en la económica del país.

En el año 2012, el grupo Enfoca SAFI se convierte en el nuevo promotor, a través de "Inversiones Educa" y "Enfoca Enseña" pasando a formar parte de una de las mayores firmas de capital privado en Perú. El grupo Enfoca SAFI se centraliza en la adquisición de empresas en sectores emergentes, con el fin de beneficiar a las mismas mediante mejoras en la gestión y crecimiento continuo, lo cual tiene por objetivo incrementar el valor de mercado de las empresas adquiridas y así obtener beneficios en el mediano y largo plazo.

En el primer trimestre del año 2012, de manera voluntaria, la Entidad inicia su proceso de autoevaluación académica con el objetivo de obtener el Certificado de Acreditación de Calidad, que es otorgado por el Consejo de Evaluación, Acreditación y Certificación de Calidad de Educación Superior No Universitaria (CONEACES) y así ofrecer el servicio educativo y de enseñanza cumpliendo adecuadamente los estándares de calidad educativa definidos por el Estado peruano. IFB Certus ha acreditado la carrera de Administración Bancaria en las Sedes Principal, San Juan y Norte, estando dentro de sus objetivos acreditar las otras 3 carreras que ofrece con el fin de lograr la excelencia y el desarrollo profesional de los jóvenes, de modo que estos puedan contribuir con el crecimiento y mejora de la competitividad del país. Entre los años 2013 y 2014, la Entidad ha tenido un crecimiento del 5% de ingresos, lo cual se constituye en un total aproximado de 15, 000 alumnos repartidos en todos los productos que ofrece la Entidad.

Como parte de los cambios promovidos por su nuevo patrocinador Enfoca SAFI en la cultura organizacional y desarrollo institucional de la Entidad, en el año 2014, se formaliza la implementación del Buen Gobierno Corporativo, el Código de Conducta y el Canal de Gestión Ética con la finalidad de que la gestión se realice con una mayor transparencia ética e íntegra.

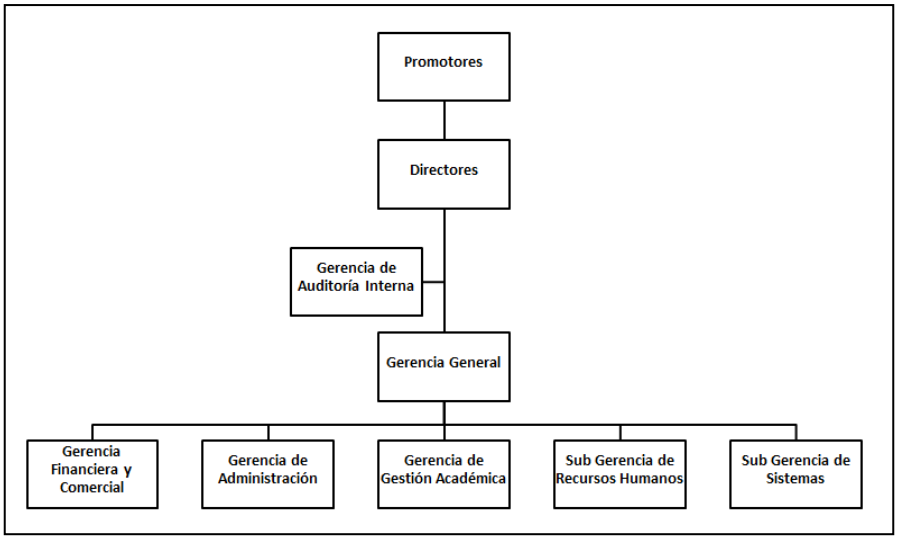
El Canal de Gestión Ética es una herramienta que sirve para comunicar anónimamente cualquier preocupación seria y sensible relacionada con potenciales irregularidades e incumplimientos del Código de Conducta del IFB Certus. Asegurando la transparencia, el IFB Certus presenta materiales que están diseñados especialmente para brindar los conocimientos en los que los usuarios pueden informarse de la garantía y confiabilidad de la Institución:

- Autorización Sistema Modular por Competencias Laborales
- Revalidación Carrera de Administración Bancaria
- Autorización Carrera de Administración Bancaria 2013
- Autorización provisional Carrera de Administración Bancaria
- Resolución Autorización Sede Principal
- Resolución Autorización Sede San Isidro
- Resolución Autorización Sede Los Olivos
- Resolución Autorización Sede Norte
- Resolución Autorización San Juan de Lurigancho
- Resolución Autorización Sede Arequipa
- Resolución Autorización Sede Chiclayo
- Autorización Carreras de Contabilidad y Negocios Internacionales Sede Arequipa
- Autorización Carreras de Contabilidad y Negocios Internacionales Sede Chiclayo

- Autorización Carreras de Contabilidad y Negocios Internacionales Sedes de Lima

La Entidad se encuentra organizada de la siguiente manera:

Gráfico 1. Organigrama de IFB Certus



Fuente: Elaboración Propia, 2015

1. Visión

La visión del Instituto es ser la comunidad educativa reconocida por la calidad de sus egresados gracias a un modelo académico de vanguardia. (*IFB Certus* 2015)

2. Misión

La misión del Instituto es formar personas de excelencia que logren sus proyectos de vida. (*IFB Certus* 2015)

3. Valores

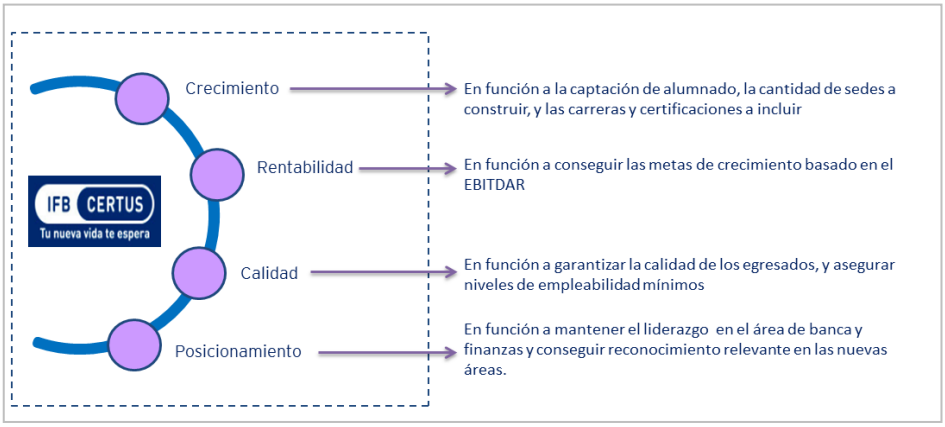
Los Valores que destaca el Instituto son:

- Transparencia: "Búsqueda de excelencia en todo lo que hacemos".
- Calidad: "Marcamos la diferencia".
- Respeto: "Sinergia y eficiencia en la gestión"
- Trabajo en equipo: "Con quiénes estamos y dónde estamos"
- Integridad: "Nuestra única opción".
- Enfoque en sus audiencias: "Nos preocupamos por lo que necesitan nuestros estudiantes y lo que requiere el mercado laboral". (*IFB Certus* 2015)

4. Objetivos estratégicos de la Entidad

La Entidad ha definido 4 criterios como sus objetivos estratégicos, respecto a la forma en que trata de crear, conservar y materializar el valor para sus grupos de interés:

Gráfico 2. Objetivos estratégicos de IFB Certus



Fuente: Elaboración Propia, 2015

En la actualidad, la Entidad se encuentra en un proceso de expansión a nivel nacional y mejora de sus procesos para la atención tanto del cliente externo como del interno; estas actividades demandan una importante inversión tanto en recursos financieros como en capital humano, generando constantes cambios en el entorno donde se desarrolla (Económico, Social o Normativo, entre otros); por tal motivo y, con el propósito de apoyar a la Entidad en sus esfuerzos por el logro de los objetivos estratégicos, se identifica la importancia de fortalecer y mantener un Sistema de Control Interno eficaz y eficiente que permita incrementar la posibilidad de su consecución.

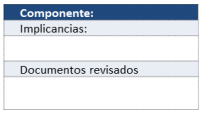
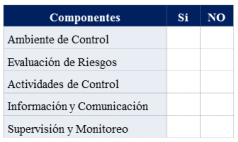
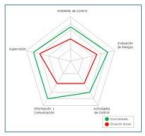
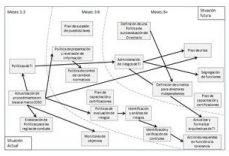
Capítulo III. Marco Teórico

Metodología para el Desarrollo del Trabajo de Investigación.

El objetivo principal del presente trabajo radica en proponer los lineamientos para fortalecer el Sistema de Control Interno sobre la base del Marco COSO 2013.

Para fijar el horizonte del trabajo y asegurar que el desarrollo de este se oriente a abordar y resolver el propósito indicado, se ha visto por conveniente definir una metodología que nos permita esquematizar en un adecuado orden los pasos a seguir a fin de contemplar los inputs necesarios para el desarrollo del trabajo de investigación.

La metodología ha sido definida en función del siguiente esquema:

1	Identificación del Marco Metodológico		Se ha visto por conveniente y adecuado el uso del marco integrado de control Interno COSO-2013, el cual se presenta a mayor detalle en el literal 2 del capítulo IV
2	Identificación de la documentación requerida para el trabajo		Se espera que la formalización de los lineamientos planteados por la Dirección de la Entidad sea formalizada a través de políticas, procedimientos y documentos guía, por lo cual se revisó el alcance de cada componente a fin de delimitar los documentos requeridos para la revisión, los que se detallan en el capítulo V
3	Entrevistas con Stakeholders (alineamiento de expectativas)		Se realizaron encuestas a los medios y altos mandos de la Entidad a fin de conocer su percepción sobre la situación actual del Sistema de Control Interno. Los resultados se presentan en el capítulo V Se realizaron también reuniones, las que tuvieron como propósito alinear expectativas respecto de los resultados esperados del trabajo de investigación
4	Diagnóstico de la situación actual		Para propósitos del trabajo de investigación se ha considerado que todos los principios son aplicables en menor o mayor medida a la Entidad. Sobre la base del marco se han evaluado los cinco componentes, los que se presentan a detalle en literal 4 del capítulo V
5	Identificación de planes de acción requeridos en función del diagnóstico		En función a los resultados del Diagnóstico se identificaron las acciones necesarias a fin de minimizar las brechas de control identificadas, para lo cual en el capítulo VII se presenta el resultado de la identificación y valoración de los planes
6	Definición de la hoja de ruta		Se definieron aquellos puntos más críticos, para los cuales se elaboraron y propusieron los planes de remediación, considerando para ello la dependencia existente entre la implementación de una acción y otra. El resultado de dicho análisis se presenta en el gráfico 5.

1. Sistema de Control Interno

De acuerdo con COSO (2013), un Sistema de Control Interno es un proceso de actividades continuas llevado a cabo por todo el personal de la organización, desde el Consejo de Administración[1] hasta las áreas operativas y de reporte. El propósito del Sistema de Control Interno es permitir que la Dirección

[1] Consejo de Administración: de acuerdo con el Marco, se entiende por este concepto al máximo órgano de gobierno, incluidos los consejeros, los socios generales, los propietarios o el consejo de supervisión.

oriente sus esfuerzos, de una forma eficaz y eficiente, en la consecución de los objetivos operativos y de desempeño financiero, así como también en reforzar la capacidad de afrontar los cambios coyunturales que se puedan producir en el entorno económico y de negocio, y manejar en forma adecuada sus prioridades y el modelo de negocio.

Otros conceptos importantes planteados como parte del Marco a ser considerados en el entendimiento del concepto de control interno son los siguientes:

- Está orientado a la consecución de los objetivos, que se clasifican en tres categorías: operacionales, de información, y de cumplimiento; pudiendo un objetivo compartir más de una categoría
- Es un medio para llegar a un fin y no un fin por sí mismo. El control interno es un proceso dinámico e iterativo que se integra en todos los procesos de una Entidad y permite sistematizar y unificar aquellos controles que pudieran desarrollarse de manera aislada a fin de obtener actividades eficientes y controladas.
- Es llevado a cabo por personas y no se acota estrictamente a la documentación y existencia de políticas y procedimientos, sino de personas y de las acciones que estas puedan ejercer en los distintos niveles de la Entidad, como parte de las tareas y actividades de control interno dentro de sus límites y responsabilidades.
- Proporciona un "aseguramiento razonable" pero no seguridad absoluta. Se reconoce que existen ciertas limitaciones por lo cual se acepta que una Entidad no va a conseguir siempre sus objetivos tanto por factores internos como ajenos a la Entidad; sin embargo, un sistema de control fortalecido incrementa la probabilidad de que la organización consiga sus objetivos.
- Es adaptable a la estructura de la organización, la definición de control interno adoptada por el Marco COSO aporta cierto nivel de flexibilidad en cuanto a la aplicación, ya que considera que esta podrá ser adecuada en función de las necesidades o circunstancias específicas de cada compañía, así como al tamaño, al sector de desarrollo, a la tecnología disponible, y al entorno de regulaciones aplicables, así como se acepta que este pueda tener matices para sus filiales, divisiones y unidades operativas o de negocio. <<Entendiendo que el sistema de control interno de una organización siempre será diferente al de cualquier otra organización>> (COSO 2013: 7)

Como parte del objetivo del presente trabajo de investigación, se ha visto por conveniente y adecuado el uso del marco integrado de control interno COSO-2013; Marco reconocido y ampliamente utilizado y aceptado como el marco líder para diseñar, implementar y desarrollar el control interno y evaluar su efectividad, de acuerdo con lo indicado por el Instituto de Auditores Internos de España (2013)

2. Marco COSO 2013

Después de casi 20 años de aplicación del Marco de Control Interno emitido por el Committee of Sponsoring Organizations of the Tradeway Commission (COSO[2]) en 1992, se emitió un nuevo Marco conocido como COSO 2013, el cual responde a las exigencias del ambiente de negocios y operativos actuales. El nuevo Marco es el resultado de aportes de distintos interesados del ambiente de negocios, firmas de auditoría, participantes en los mercados financieros y estudiosos del tema.

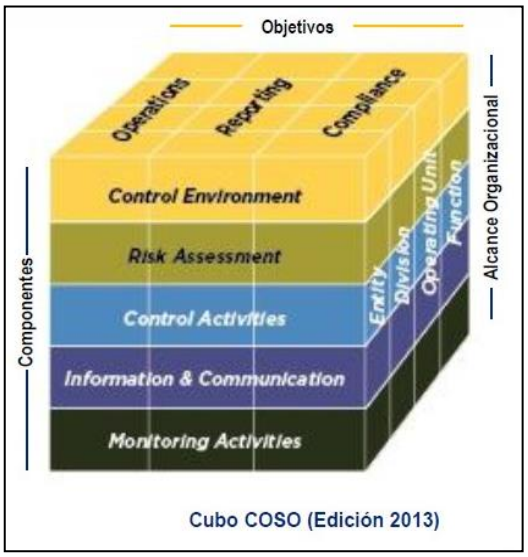
La actualización del Marco responde principalmente a los cambios empresariales y operativos ocurridos en los últimos años, tales como la globalización, la mayor complejidad en las actividades empresariales, la dependencia de la tecnología, y el mayor interés en la prevención y la detección del fraude, entre otros. La actualización considera también la ampliación de la evaluación en cuanto a los objetivos de reporte financiero, no financiero y de reporte interno. De acuerdo con COSO (2013) este Marco de Control Interno incrementa la probabilidad de cumplimiento de los objetivos de la entidad, mediante el desarrollo eficiente y efectivo, así como el mantenimiento continuo de un Sistema de Control Interno fortalecido.

El Marco contempla tres categorías de objetivos, cinco componentes, y cuatro niveles de estructura de la organización, los que están inmersos en una relación directa entre lo que se espera lograr, lo que se requiere para lograrlo y el cómo se involucra a los diferentes niveles de la organización.

La representación gráfica del Marco es un cubo en el que las categorías de objetivos están representadas por columnas, los componentes por filas y los niveles de estructura organizacional por la tercera dimensión del cubo.

[2] COSO es una iniciativa del sector privado, patrocinado y financiado conjuntamente por: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (FEI), Institute of Management Accountants (IMA), The Institute of Internal Auditors (IIA).
Se dedica a proporcionar el desarrollo de nuevos marcos y orientaciones generales sobre el control interno, la gestión del riesgo empresarial, y disuasión de fraude, diseñado para propiciar la mejora del desempeño organizacional y la supervisión, así como la reducción del riesgo de fraude en las organizaciones.

Gráfico 3. Marco COSO 2013



Fuente: COSO Integrated Framework Executive Summary, Mayo 2013.

2.1 Categorías de Objetivos

El definir los objetivos es un pilar básico no solo para la planificación estratégica sino que es un requisito y punto de partida para el establecimiento de un Sistema de Control Interno. En función de la perspectiva de negocio, continuidad y futuro de cada Compañía se establece la misión, visión y estrategias de la organización, lineamientos que representan el camino que la Dirección ha definido como la forma de crear, materializar y conservar el valor para sus *stakeholders*. Por otro lado, la relación no puede ser inversa, es decir, la definición, selección y estructuración de objetivos no forma parte del control interno.

Estos objetivos pueden ser de cualquier índole, siempre y cuando estos sean <<específicos, medibles u observables, alcanzables, relevantes y limitados en el tiempo>> (COSO 2013: 8) con la finalidad de que puedan ser comprendidos por aquellas personas que se encuentren involucrados directamente en la consecución de los mismos.

El Marco COSO define la agrupación de los objetivos en tres categorías:

2.1.1 Objetivos Operacionales:

Relacionados con el cumplimiento de la misión y visión de la organización. La falta o inadecuada definición de estos podría repercutir en una subutilización de recursos.

Como parte de estos objetivos, el Marco COSO incluye también la salvaguarda, el mantenimiento y eficiente uso de los bienes de una organización.

2.1.2 Objetivos de Información:

Vinculados a la preparación de informes de utilidad para uso interno y externo de los *stakeholders*, pudiendo estar relacionados con la información financiera, no financiera, interna o externa.

En cuanto a información interna, los objetivos se definen en respuesta a las necesidades o potenciales necesidades tales como planificación operativa, decisiones estratégicas y evaluación del desempeño, entre otros temas a ser evaluados por la organización.

En cuanto a información externa, los objetivos se definen en respuesta a la regulación y normas aplicables en razón de parámetros normalizados aplicables a la organización. Tales como los estados financieros o los informes de cumplimiento en relación con una ley aplicable.

2.1.3 Objetivos de Cumplimiento:

Relacionados con el conjunto de parámetros de cumplimiento esperados en función de las leyes, reglas y regulaciones aplicables a la organización.

2.2 Componentes del Marco

Para los cinco componentes, como parte del Marco se han definido también 17 principios y 87 puntos de enfoque[3] que enfatizan y disgregan el alcance de cada componente. Los componentes definidos son:

2.2.1 Entorno de Control:

La definición del entorno de control según el Marco COSO (2013), es el conjunto de normas, procesos y estructuras que proveen las bases para llevar a cabo el control interno en la Entidad. El Directorio y la Alta Dirección establecen la filosofía respecto a la importancia del control interno y las normas de conducta esperadas, considerando la integridad y los valores éticos de la Entidad.

Los principios involucrados en este componente son los siguientes:

- La organización demuestra compromiso con la integridad y los valores éticos.
- El Consejo de Administración demuestra independencia de la Dirección y ejerce la supervisión del desempleo del Sistema de Control Interno

[3] <<Los puntos de enfoque o puntos de interés constituyen importantes características de los principios, sin embargo el Marco no requiere que la Dirección evalúe por separado si estos puntos de interés se encuentran presentes>> (COSO 2013:20). <<La Dirección puede determinar que algunos de estos puntos de interés no son adecuados o relevantes y puede identificar y tener en cuenta otros puntos de interés con base en las circunstancias específicas de la organización>> (COSO 2013:26)

- La Dirección establece, con la supervisión del Consejo, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.
- La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes en alineación con los objetivos de la organización.
- La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.

2.2.2 Evaluación de Riesgos

De acuerdo con la definición del Marco COSO (2013), se entiende que la evaluación de riesgos es un proceso dinámico que considera la evaluación de los riesgos en función de los niveles de impacto que estos pudiesen tener sobre el logro de los objetivos definidos para todos los niveles de la organización, sobre todo si estos impactan adversamente a la Entidad.

Los principios involucrados en este componente son los siguientes:

- La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.
- La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la organización y los analiza como base sobre la cual determinar cómo se deben gestionar.
- La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.
- La organización identifica y evalúa los cambios que podrían afectar significativamente al Sistema de Control Interno.

2.2.3 Actividades de Control

De acuerdo con la definición del Marco COSO (2013), las actividades de control corresponden a los lineamientos establecidos por la organización mediante la formalización de políticas y procedimientos que tienen por objetivo difundir las instrucciones de la Dirección con respecto a las acciones a tomar a fin de mitigar los riesgos que impacten en el logro de los objetivos.

Las actividades de control se ejecutan en todos los niveles de la organización, a nivel de procesos y actividades soportadas en tecnología de la información, entre otros. De acurdo con la clasificación, según su naturaleza, los controles pueden ser clasificados como preventivos o detectivos, así como manuales y automáticos.

Los principios involucrados en este componente son los siguientes:

- La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.
- La organización define y desarrolla actividades de control a nivel de organización sobre la tecnología para apoyar la consecución de los objetivos.
- La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y los procedimientos que llevan dichas políticas a la práctica.

2.2.4 Información y Comunicación

De acuerdo con la definición del Marco COSO (2013), la información es necesaria para la Entidad a fin de que esta pueda ejercer las responsabilidades de control interno para la consecución de los objetivos. La comunicación se realiza de forma interna y externa, permitiendo a los colaboradores comprender la filosofía de la Alta Dirección respecto al control interno así como las responsabilidades del control y su necesidad e importancia para el logro de los objetivos.

Los principios involucrados en este componente son los siguientes:

- La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.
- La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.
- La organización se comunica con las partes interesadas externas sobre los aspectos clave que afectan al funcionamiento del control interno.

2.2.5 Actividades de Supervisión

De acuerdo con la definición del Marco COSO (2013), son las evaluaciones continuas e independientes, con la finalidad de determinar si cada uno de los componentes del control interno se encuentran presentes y funcionando eficientemente. Los hallazgos son evaluados y las deficiencias son comunicadas al Directorio (Comité de Auditoría) y a la Alta Dirección, oportunamente.

Los principios involucrados en este componente son los siguientes:

- La organización selecciona, desarrolla y realiza evaluaciones continuas e independientes para determinar si los componentes del Sistema de Control Interno están presentes y en funcionamiento.
- La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la Alta Dirección y el Consejo, según corresponda.

2.3 Niveles de la estructura de la organización

Para el Marco COSO (2013), la estructura de la organización que incluye las divisiones, filiales, unidades operativas y funcionales, se puede clasificar a nivel de:

- Organización
- División
- Unidad Operativa
- Función

3. Efectividad del Control Interno

Un Sistema de Control Interno se determina como efectivo en el caso de que los componentes se encuentren presentes y en funcionamiento, y que los cinco componentes funcionen juntos de forma integrada>> (COSO 2013:20). Al poder determinar cómo efectivo el sistema de Control Interno, la Entidad contará con seguridad razonable acerca del cumplimiento de los objetivos en las tres categorías pautadas por el Marco: Operacional, de Información y de Cumplimiento.

En cuanto a eficacia, el Marco COSO no establece el proceso sobre cómo la Dirección debe evaluar su eficacia, ya que este concepto se encuentra más asociado a la Gestión Integral de Riesgos. .

En cuanto a las deficiencias de control, de acuerdo con el Marco COSO (2013) estas hacen referencia a la falta de uno o más componentes, así como de los principios relevantes que de ellos se desprenden, lo cual reduce la probabilidad de que la Entidad pueda cumplir con sus objetivos.

La gravedad de las deficiencias de control estará directamente relacionada con la severidad de la probabilidad[4] de incumplimiento de los objetivos de la Entidad. Al existir una deficiencia de control severa, la Entidad no podrá concluir que se cuente con un Sistema de Control Interno efectivo.

En adición, con respecto al incumplimiento de un principio, es importante señalar que los principios son complementarios pero no reemplazables, es decir si la Entidad identifica una deficiencia grave o severa en relación con un principio, esta no puede ser minimizada o controlada a través de la presencia y funcionamiento de otro principio o principios.

En función de lo descrito en el presente capítulo, y con la finalidad de cumplir con el primer objetivo del Trabajo de Investigación, y determinar el nivel de madurez del sistema de control interno de la Entidad utilizando como referencia el Marco COSO 2013, en el siguiente capítulo se presenta el Diagnóstico de

[4] <<El Marco contempla el uso del criterio profesional a la hora de evaluar el impacto potencial de una deficiencia de control en la presencia y el funcionamiento de un principio relevante>> (COSO 2013: 27)

la situación actual, el cual se ha realizado en base al criterio profesional[5] y a partir de la evaluación de los principios y componentes del Sistema de Control Interno, tomando en consideración su relación con los objetivos y niveles de organización establecidos por el Marco COSO, tanto a nivel de presencia como de funcionamiento, ya que si el control interno se determina como efectivo, la organización podrá contar con cierta seguridad razonable en relación con el cumplimiento de los objetivos operacionales, de información y de cumplimiento.

[5] <<El Marco requiere la aplicación del criterio profesional a la hora de diseñar, implementar y ejecutar el sistema de control interno y evaluar su eficacia. El uso de dicho criterio profesional mejora la capacidad de la dirección para tomar mejores decisiones sobre el sistema de control interno. Pero no puede garantizar resultados perfectos>> (COSO 2013: 25)

Capítulo IV. Diagnóstico de la situación actual de la Entidad en relación con el marco teórico seleccionado

1. Revisión de la documentación existente

Se espera que la formalización de los lineamientos planteados por la Dirección de la Entidad sea formalizada a través de políticas, procedimientos y documentos guía, ya que estos permiten acotar y definir responsabilidades así como plasmar la visión de la Dirección en referencia al actuar de la organización con respecto al desarrollo del control interno. A su vez, los procedimientos definen a través de medidas y acciones específicas el cómo implementar las políticas.

De acuerdo con el Marco COSO (2013), una documentación eficaz posibilita una adecuada estructuración del diseño del control interno, delimita expectativas de desempeño y conducta y permite comunicar dinámicamente las responsabilidades a nivel de quién, qué, cuándo, dónde y porqué se debe realizar el control interno. Teniendo en cuenta que una adecuada documentación permite fortalecer las pruebas de la ejecución del control interno, y en función del alcance del análisis requerido para la evaluación de los 87 puntos de enfoque[6], se identificaron los documentos oportunos para la revisión a ser solicitados a la Entidad para la evaluación y diagnóstico del nivel de madurez de cada componente. Los documentos revisados son los que se mencionan a continuación:

Tabla 1. Relación de documentos revisados por componente COSO 2013

Componente	Documentos revisados
Ambiente de Control	• Declaraciones de la misión, visión y valores de la Entidad • Código de Conducta/ética • Directivas relacionadas con la comunicación descendente • Lineamientos sobre la respuesta a las actitudes o desviaciones al Código de Conducta • Listado de los comités vigentes y documentos que sustenten su funcionalidad • Organigrama vigente • Lineamientos para la delegación de autoridad • Documentación relacionada con los niveles de segregación de funciones definidos

[6] El detalle de los 87 puntos de enfoque se presenta en el Anexo 2

	• Políticas de recursos humanos definidas para la contratación • Manuales de organización y funciones
Evaluación de riesgos	• Lineamientos de evaluación de riesgos • Lista de los objetivos de la Entidad • Lista de estrategias en relación con los objetivos • Lista de los riesgos identificados a nivel Entidad y a nivel operacional • Consideraciones para la evaluación de fraude • Política de línea ética
Actividades de Control	• Políticas y procedimientos para la documentación de controles • Lista de los riesgos identificados a nivel Entidad y a nivel operacional • Documentación relacionada con los niveles de segregación de funciones definidos • Procedimientos de delegación de autoridad • Inventario de sistemas de TI utilizados
Información y Comunicación	• Matrices de riesgos y controles • Inventario de sistemas de TI utilizados • Políticas y procedimientos para la documentación de controles • Políticas y procedimientos para el tratamiento y gestión de la línea ética • Procedimientos de comunicación interna y externa
Actividades de supervisión	• Lineamientos de evaluación de riesgos • Listado de controles identificados por la Entidad

Fuente: Elaboración Propia, 2015

2. Encuesta de los elementos de control interno

El objetivo de esta encuesta anónima es conocer la percepción del personal respecto del entendimiento y difusión del control interno, así como del nivel de aplicabilidad desde la percepción de cada unidad operativa.

El alcance considera la evaluación del Sistema de Control actual vinculado a los cinco componentes del Marco COSO 1992 (Ambiente de Control, Evaluación de Riesgo, Actividades de Control, Información y Comunicación; y Monitoreo y Supervisión así como los principios respectivos). Cabe mencionar, la selección de este Marco fue debido a que en el año 2013, la Entidad inició las actividades para el fortalecimiento del Sistema de Control Interno y, a su vez, las capacitaciones al personal fueron brindadas bajo este marco.

Considerando la importancia que da el Marco COSO 2013 al "*Tone at the Top*" respecto al control interno y los estándares de conducta esperados dentro de la Entidad, los participantes dentro de esta encuesta anónima fueron las gerencias de línea y sus respectivas jefaturas. Es importante precisar lo siguiente:

- La encuesta es de carácter anónimo para que las respuestas no sean influencias por la Alta Dirección o similares.
- La Alta Dirección ha empoderado a las gerencias de línea respecto a las actividades de control interno.
- Se sugirió a las gerencias de línea y jefaturas, antes de responder el cuestionario, tener reuniones con sus equipos de trabajo y recopilar sus opiniones sobre la base de las preguntas formuladas.

Esta encuesta se ejecutó a través de la herramienta *Google Drive*, propia de la Entidad, que facilitó la votación anónima de los encuestados y así se obtuvo la valoración por cada componente, además de comentarios que permitieron identificar puntos de atención oportunos para así lograr un mejor enfoque de la revisión documentaria. Respecto a la valoración por cada componente, todos los componentes tienen una valoración aritmética dándoles la misma importancia.

Como parte del trabajo de investigación se revisaron las respuestas y los porcentajes de calificación a fin de identificar cómo estos calzan y aplican con los focos definidos en el Marco COSO 2013. A continuación, presentamos los resultados obtenidos de la encuesta realizada:

Tabla 2. Resumen: evaluación de los elementos de control interno – cuestionario COSO

Elementos de Control Interno	NO		SÍ	
	2014	2015	2014	2015
Ambiente de Control	33%	34%	67%	66%
Evaluación de Riesgos	46%	38%	54%	63%
Actividades de Control	38%	36%	62%	64%
Información y Comunicación	39%	29%	61%	71%
Supervisión y Monitoreo	28%	33%	72%	67%

Fuente: Elaboración propia en base al marco COSO 1992 (2015)

Tabla 3. Evaluación de los elementos de control interno – cuestionario COSO (percepción del personal respecto de la existencia de los elementos de control interno)

Categorías	Preguntas	Cumple	
		Sí	No
Ambiente de Control			
Filosofía de la Dirección	- La Gerencia muestra interés en establecer un adecuado control interno, proporcionando apoyo logístico y de personal, para un adecuado desarrollo de las labores de control. - Existen mecanismos de difusión que permitan al personal aumentar sus conocimientos referidos a los controles internos del IFB CERTUS.	68%	32%
Integridad y valores éticos	- La Gerencia se conduce de acuerdo con los principios y valores éticos. - Existe un Código de Conducta y una declaración de valores. - Existen mecanismo de denuncias anónima. - La Gerencia se asegura que los trabajadores conozcan los documentos normativos que regulan las actividades del IFB CERTUS.	82%	18%
Administración estratégicas	- Existe una adecuada difusión de la visión, misión, metas y objetivos estratégicos. - La elaboración, actualización y difusión de los planes estratégicos es realizada según el procedimiento documentado.	77%	23%
Estructura Organizacional	- Se difunde de manera correcta la estructura organizacional del IFB CERTUS. - Las actividades de todos los colaboradores se encuentran debidamente delimitadas y documentadas en el MOF.	58%	42%
Administración de Recursos Humanos	- En el IFB CERTUS se evalúa y revisa periódicamente al desempeño laboral de cada empleado. - Gestión del Talento Humano vela porque cada área cuente con la cantidad de personal adecuada y elabora un plan de capacitación para los empleados - La escala remunerativa es acorde con el cargo desempeñado.	54%	46%
Competencias Profesional	- Se han identificado las competencias necesarias para cada cargo de la Entidad, las cuales han sido plasmadas en un documento formal (perfiles de cargo). - El personal que ocupa cada puesto de trabajo cuenta con las competencias establecidas o requeridas por los perfiles del cargo.	56%	44%

Categorías	Preguntas	Cumple	
		Sí	No
Ambiente de Control			
Asignación de autoridad y responsabilidad	- El personal conoce sus responsabilidades y actúa de acuerdo con los niveles de autoridad que le corresponden. - La autoridad y responsabilidad del personal están claramente definidas en los manuales, reglamentos y otros documentos normativos, los cuales son actualizados y difundidos periódicamente al personal.	64%	36%
Opinión del Personal		**66%**	**34%**
Evaluación de Riesgos			
Planeamiento de la Adm. riesgos	- Se ha desarrollado un Plan de Administración de Riesgos en donde se incluyen las actividades de identificación, valoración, respuesta, monitoreo y documentación de riesgos.	61%	39%
Identificación de los riesgos	- La Gerencias ha participado en la identificación de los riesgos que afectan a la Entidad y estos han sido documentados tanto a nivel de entidad como a nivel de procesos.	73%	27%
Valoración de los riesgos	-Se realiza periódicamente una evaluación de riesgos y se ha calificado y priorizado según su probabilidad e impacto. Considera que los riesgos se encuentran correctamente documentados	58%	42%
Respuesta al riesgos	- Existe estrategias de respuesta al riesgo definidas por la Alta Dirección para la gestión de los mismos.	58%	42%
Opinión del Personal		**63%**	**37%**
Actividades de Control			
Segregación de funciones	- Se han definido, actualizado y difundido procedimientos de aprobación y autorización para las actividades y tareas realizadas en los procesos de la Entidad - Se identifican las actividades potencialmente expuestas a riesgos de error o fraude. - Se realiza rotación de personal	73%	27%
Evaluación Costo – Beneficio	- El IFB CERTUS ha realizado un análisis costo - beneficio de los controles que tienen establecidos, lo cual podría indicar que existen controles ineficientes.	48%	52%
Controles sobre los recursos	- En el IFB CERTUS se realizan verificaciones periódicas respecto de la ejecución de las actividades (concilian de registros). - Se han establecido políticas y procedimientos relacionados con el uso y protección de los recursos de información.	73%	27%
Evaluación de desempeño e indicadores	- El IFB CERTU cuenta con indicadores de desempeño para los procesos, actividades y tareas, orientados a medir los resultados individuales y a nivel de toda la Organización. - Se cuenta con políticas y procedimientos actualizados y difundidos para la rendición de cuentas.	70%	30%

Categorías	Preguntas	Cumple	
		Sí	No
Ambiente de Control			
Documentación y revisión de procesos	- El personal del IFB CERTUS conoce qué procesos involucran a su área y qué rol le corresponde en los mimos. - IFB CERTUS ha adoptado un enfoque de procesos riesgos-controles, así como que los procesos del Instituto estén documentados y actualizados.	61%	39%
Controles para las TIC	- Se han creado perfiles de usuarios acordes con las funciones desempeñadas. - Se cuenta con políticas y procedimientos documentados para la administración de los sistemas de información, con planes operativos, informáticos y de contingencia.	61%	39%
Opinión del Personal		**64%**	**36%**
Información y Comunicación			
Funciones características y responsabilidad de la información	- Se ha asignado a uno o más miembros de Gerencia para responder de forma apropiada a los clientes, proveedores, entidades, etc. - La información gerencial es adecuadamente procesada y proporcionada para la toma de decisiones.	70%	30%
Calidad y suficiencia de la información	- La información tanto interna como externa que maneja el IFB CERTUS es útil, oportuna, transparente y confiable y se realiza la retroalimentación a los usuarios para priorizar las mejoras correspondientes en el sistema.	82%	18%
Sistemas de Información	- IFB CERTUS se encuentra integrado a un solo sistema de información, que se ajusta a la necesidad del mercado. - Se realiza la retroalimentación a los usuarios para priorizar las mejoras correspondientes en el sistema.	77%	23%
Flexibilidad al cambio	- Se realizan revisiones periódicas de los sistemas de información, mediante las cuales se solicita retroalimentación a los usuarios con la finalidad de rediseñar o modificar los sistemas en busca de un adecuado funcionamiento a satisfacción de las necesidades.	36%	64%
Confidencialidad de la información	- El IFB CERTUS ha determinado procedimientos adecuados que salvaguardan la confidencialidad de la información relacionada principalmente al área Comercial y de Desarrollo	73%	27%
Comunicación interna y externa	- Se ha elaborado y difundido políticas o lineamientos que orienten la comunicación interna. Se cuenta con mecanismos y procedimientos adecuados para brindar información hacia el exterior.	80%	20%
Asignación de autoridad y responsabilidad	- Se han implementado políticas que estandarizan la comunicación interna y externa, considerándose diversos tipos de comunicación: memorandos, paneles informativos, boletines, revistas, correos electrónicos reiterativos, entre otros.	82%	18%
Opinión del Personal		**71%**	**29%**
Monitoreo			
Prevención y monitoreo	- El IFB CERTUS realiza acciones de supervisión para conocer oportunamente si las actividades del Instituto se efectúan de acuerdo con lo establecido, dejando	67%	33%

Categorías	Preguntas	Cumple	
		Sí	No
Ambiente de Control			
	evidencia de dichas acciones de supervisión.		
Opinión del Personal		**67%**	**33%**

Fuente: Elaboración propia en base al Marco COSO 1992 (2015)

De los resultados mostrados en los cuadros anteriores y como fruto del análisis de esta encuesta se identificó lo siguiente:

- Los encuestados reconocen la existencia de la documentación; sin embargo, creen que esta no ha sido difundida a un nivel necesario para que pueda ser interiorizada como propia por cada una de las áreas operativas de la Entidad.
- Desconocimiento por parte del personal de las estrategias definidas por la Gerencia para la difusión, normativa y normalización del control interno.
- Con respecto a la evaluación del componente de ambiente de control, casi el 50% del personal encuestado indica estar disconforme con las políticas y procedimientos de evaluación de desempeño. Reconocen también que, si bien se tienen identificadas las funciones y responsabilidades por puesto definido a nivel documentario, estas no se alinean a la realidad de las funciones que el personal debe realizar.
- Se identifica también, a partir de las respuestas, que el personal considera que la responsabilidad y autoridad no es asumida totalmente por los responsables designados para ello.
- Con respecto al análisis del componente de evaluación de riesgos, alrededor del 50% del personal discrepa de la realizada, y opina que los riesgos no se encuentran correctamente documentados y calificados. Por otro lado, el personal reconoce que si bien la Gerencia gestiona las respuestas al riesgo, estas no son desarrolladas de acuerdo con el alcance con el que inicialmente fueron definidas.
- Con respecto a la evaluación del componente de Actividades de Control, más del 50% del personal considera que la Entidad no ha realizado un análisis de coste beneficio para la definición de las actividades de control. Por otro lado, más de un tercio del personal considera que no se cuenta con políticas y procedimientos para la administración de los sistemas de información, y que los perfiles a nivel de sistemas no se encuentran acorde con las funciones desempeñadas. En adición, el personal reconoce que no se cuenta con planes de contingencia en caso de inconvenientes tecnológicos.
- Si bien la percepción con respecto al componente de Información y Comunicación ha mejorado respecto del año anterior, más del 50% del personal encuestado considera que no se realiza el análisis de retroalimentación con respecto de los sistemas de tecnología actuales, a fin de recoger la

percepción del usuario para la mejora y rediseño de los sistemas, y que estos puedan orientarse a sus necesidades.

- La ponderación de la calificación del componente de Monitoreo aumentó en 5% con respecto al año anterior; sin embargo, un tercio del personal encuestado se encuentra en desacuerdo con la afirmación de que la Entidad realiza acciones de supervisión para conocer si las actividades de la Entidad se efectúan conforme a lo establecido, dejando evidencia de dichas acciones.

3. Entrevista con la Alta Dirección y el Auditor Interno

Obtenidos los resultados de la encuesta "Evaluación de los Elementos de Control - Cuestionario COSO" que contiene la percepción del personal sobre la existencia de los elementos de control interno, procedimos a tener una entrevista con la Alta Dirección y el Auditor Interno de la Entidad con la finalidad de conocer su opinión sobre:

a) Importancia del Sistema de Control Interno en la Entidad
b) Grado de madurez del Sistema de Control Interno de la Entidad según componentes
c) Valor agregado del Sistema de Control Interno
d) Resultado de la encuesta realizada

De las entrevistas efectuadas, se recogieron principalmente los siguientes puntos:

a) La Entidad ha realizado grandes esfuerzos para mejorar su Sistema de Control, como cambio en el ERP *PeopleSoft* y mejora de los procesos internos, con la finalidad de dar soporte al crecimiento de la Entidad; sin embargo, esta acción se encuentra en proceso debido a que estas actividades se iniciaron en el año 2013 y se estima la finalización en un mediano o largo plazo.
b) Con ayuda de la "Tabla de ponderación para la evaluación del nivel de madurez de los componentes de COSO" que figura en el Anexo 1 del presente trabajo, los entrevistados indicaron que la Entidad tiene un grado de madurez nivel 2 "En proceso de implementación" debido a que algunos componentes de control interno se encuentran definidos de manera general pero no se han definido ni parametrado los ámbitos para su aplicación; por ejemplo, a inicios del año 2014 se creó la Gerencia Comercial con la finalidad de centralizar y estructurar la gestión comercial de la Entidad para que se realice recolección y análisis de información con respecto al mercado objetivo. Por otro lado, se cuenta con políticas que regulan los procesos existentes; sin embargo, dada la implementación de los dos nuevos sistemas que soportan la parte comercial y operativa de la Entidad, la actualización de dichos procesos se encuentran en curso debido a la mejora de los procesos.
c) Ambos entrevistados indicaron que un eficiente Sistema de Control Interno permite identificar las deficiencias de control de manera oportuna y la comunicación a los responsables de realizar

acciones correctivas. Asimismo, permite tomar medidas antes de que pudiesen afectar de manera significativa el logro de objetivos.

d) Si bien los resultados arrojan una mejora en comparación al año 2014, indicaron que es necesario dar mayor énfasis al proceso de sensibilización y capacitación del personal de la entidad sobre el Sistema de Control Interno y sus componentes. Este proceso es parte del cambio de la cultura organizacional que se viene dando desde el año 2013.

4. Análisis del nivel de madurez con respecto al marco teórico COSO 2013

El Marco COSO 2013 establece como marco para el Sistema de Control Interno cinco componentes y 17 principios, los que definen los conceptos fundamentales de dicho Marco. Para los propósitos de este trabajo de investigación se ha considerado que todos los principios son aplicables en menor o mayor medida a la Entidad, ya que como se indica en el Marco COSO <<Estos componentes y principios del Sistema de Control Interno son aplicables para todas las organizaciones>> (COSO 2013:14). Se indica también, que <<Los principios son conceptos fundamentales asociados con los componentes. Como tales, el Marco considera que los 17 principios son adecuados para todas las organizaciones. El Marco considera que los principios son relevantes porque tienen una influencia significativa en la presencia y el funcionamiento de un componente asociado. Por consiguiente, si un principio relevante[7] no se encuentra presente[8] y en funcionamiento[9], el componente asociado no puede estar presente y en funcionamiento>> (COSO 2013:21)

Sobre la base que establece el Marco, donde se indica que se requiere que los cinco componentes funcionen juntos de forma integrada (COSO 2013:21) se han evaluado los componentes en función de los 87 puntos de enfoque, y las posibles deficiencias de control. Para cuantificar el resultado del nivel de madurez, se empleó como base la tabla de ponderación propuesta por el Marco COSO-ERM, la cual fue modificada sobre la base de criterio experto y del conocimiento de la Entidad y del tipo de negocio al que esta pertenece. El detalle de los criterios considerados se presenta en el Anexo 1.

El resultado se desarrolla a detalle a través del esquema establecido en la herramienta de evaluación definida por el Marco y documentada en la tabla 1. Los principales puntos de atención del diagnóstico se presentan a continuación por cada uno de los componentes y principios del Marco:

[7] <<La Dirección debe respaldar su determinación de que un principio no sea relevante, bajo el razonamiento de cómo, en ausencia de dicho principio, el componente asociado puede estar presente y en funcionamiento>> (COSO 2013:21)

[8] Presente: de acuerdo con el Marco Coso (2013) se entiende por presente a la existencia del componente o principio en cuanto a diseño e implementación con respecto al Sistema de Control Interno para la consecución de los objetivos especificados

[9] Funcionamiento: de acuerdo con el Marco Coso (2013) se entiende por funcionamiento que los componentes o principios siguen existiendo en el manejo del Sistema de Control Interno para la consecución de los objetivos especificados

4.1 Entorno de Control

P1: La organización demuestra un compromiso con los valores de integridad y ética.

El análisis de este principio se enfoca en que la Entidad debe demostrar su compromiso con la integridad y los valores éticos. La Entidad no ha documentado formalmente las funciones ni las responsabilidades del Comité de Directorio, Comité de Gerencia y Comité de Auditoría. Con relación a la evaluación y monitoreo del desempeño, la Entidad ha definido que este parámetro sea evaluado a través de la percepción de la Gerencia y de una evaluación de 360 grados. Con respecto al alcance de la evaluación se identificó que, si bien se evalúa el cumplimiento con respecto a objetivos a nivel operativo, no se incluyen objetivos de cumplimiento de las normas y procedimientos, por tanto, estos factores no son considerados en la evaluación de manera objetiva. Respecto a abordar cualquier desviación de forma oportuna, la Alta Dirección ha implementado en el año 2014 el canal de Gestión Ética a través del cual se reportan las situaciones relacionadas con cualquier desviación del Código de Conducta; sin embargo, este no se encuentre activo para los alumnos de las sedes de provincias y proveedores. En las encuestas a gerencias y jefaturas, declararon no conocer la existencia de un Código de Ética, y de principios y valores establecidos por la Entidad.

P2: La Junta Directiva demuestra la independencia de gestión y ejerce la supervisión de la evolución y los resultados de los controles internos.

El análisis de este principio se centra en que la interacción de Auditoría Interna con el Comité de Auditoría debe ser suficiente para determinar la independencia así como contar con la documentación que evidencie una supervisión suficiente del control interno por parte del Comité. Como se indicó en el principio 1, no se han documentado formalmente las funciones de cada Comité, sin embargo, se conocen y reconocen los objetivos de funcionamiento.

El Directorio de la Entidad se encuentra conformado por profesionales altamente capacitados, con experiencia en diversos sectores económicos y formación moral necesarios para entender las actividades de la empresa dentro del sector con la finalidad de evaluar adecuadamente y dirigirla con éxito en el largo plazo; sin embargo, la Entidad no cuenta con una política de autoevaluación del Directorio donde se defina la periodicidad a evaluar a los Directores vigentes, así como el grado de cumplimiento de las tareas durante el periodo evaluado y además, los aspectos y tareas a cumplir en el siguiente periodo. Si bien actualmente se cuenta con más de un tercio de directores independientes, dicha cuota no se encuentra oficializada, por lo cual se encuentra susceptible a variaciones. Por otro lado, la Entidad no cuenta con una definición de independencia ni con criterios definidos a ser considerados en el perfil de los directores independientes.

P3: La Dirección establece, con la supervisión del Directorio, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.
El análisis de este principio se encuentra enfocado en la gestión, a través de la Alta Dirección y Recursos Humanos, respecto a evaluar si las responsabilidades se asignan adecuadamente para establecer la rendición de cuentas.

En las entrevistas con las gerencias y jefaturas de la Entidad se relevó que se tiene una ligera percepción de que la elaboración, la actualización y la difusión de los planes estratégicos no se realizada de acuerdo con procedimientos formalmente documentados. Se identificó también que si bien existe parcialmente documentación formal sobre la organización y funciones por puesto, el problema radica en el empoderamiento y *ownership* de las jefaturas, que no interiorizan la responsabilidad por el accionar del personal a su cargo. En el año 2014, la Entidad ha implementado un nuevo ERP, tanto para el *back* como para el *front office*, por lo cual, si bien existen Manuales de Organización y Funciones (MOF), estos no han sido en su totalidad actualizados en función de los cambios que representa el pase a producción del ERP.

En cuanto a definir, asignar y limitar facultades y responsabilidades observamos lo siguiente:

- Comité de Directorio: no se encuentran formalmente documentadas las responsabilidades, sin embargo, como se desarrolló en el principio 1 en la documentación revisada se encontró evidencia de la ejecución de sus funciones.
- Alta Dirección y Personal: actualmente el Directorio y la Alta Dirección han definido las responsabilidades y límites de autoridad para todos los niveles jerárquicos, dejándolos plasmados en el Manual de Organización y Funciones (MOF). Sin embargo, al existir un cambio después de la implementación del ERP, en muchos casos, se identifica una desactualización con respecto a las funciones y responsabilidades, generando confusión en el personal sobre el alcance de estas.
- Proveedores: en los contratos celebrados, no existen cláusulas en los contratos de servicios o acuerdos firmados por ambas partes en las que se especifique las expectativas de cada parte y las responsabilidades frente a los servicios prestados, así como las responsabilidades y condiciones de los proveedores frente a los niveles de control interno sobre los procesos o actividades del negocio subcontratadas.

P4: La Organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes alineados con los objetivos de la Organización.

El análisis de este principio se centra en que la Organización necesita demostrar su compromiso de atraer, desarrollar y retener a personas competentes que también aceptan el compromiso ético de la Organización. Asimismo, este compromiso no debe cambiar en momentos difíciles.

Se reconoce que la Entidad evalúa y revisa periódicamente el desempeño laboral de cada empleado, los encuestados manifiestan que no existen adecuados procedimientos para la gestión de recursos humanos, identificándose que no se cuenta con la cantidad de personal adecuado, no se elabora o difunde un plan de capacitación para los empleados, la escala remunerativa no se encuentra acorde con el cargo desempeñado. Asimismo, se percibe que el personal que ocupa cada cargo de trabajo cuenta con las competencias establecidas o requeridas por los perfiles de cargo, sin embargo, el 44% desconoce o no reconoce que dichas competencias se desarrollen del todo.

No existe una política formalmente definida para la retención de personal calificado. Sin embargo, en función de cada caso en particular que solicita la renuncia voluntaria y en función de la evaluación de la Gerencia General en coordinación con la Gerencia responsable y Jefatura directa, se analiza el caso y la posibilidad de retención. En función de ello, se plantean al colaborador los beneficios o cambios de condiciones económicas o de desarrollo profesional.

No se cuenta con una estrategia de gestión del talento, en la que se definan y formalicen los planes de sucesión para las gerencias, subgerencias y jefaturas. No se cuenta tampoco con candidatos identificados para la sucesión y formación en caso de puestos críticos, así como también se carece de un plan de desarrollo individual y un programa de liderazgo.

P5: La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.

El análisis de este principio se concentra en que la organización necesita un mecanismo para mantener al personal responsable del control interno y, a su vez, el mecanismo se encuentre documentado. La Entidad ha definido una estructura matricial. En cuanto a la responsabilidad y *ownership* de la Gerencia y la Alta Dirección frente al control interno, se observa que las funciones y responsabilidades de cada puesto, se encuentran documentadas en el Manual de Organización y Funciones (MOF); sin embargo, este no ha sido actualizado en función de los cambios coyunturales surgidos principalmente por la implementación de los nuevos sistemas informáticos. En adición, el personal no se siente comprometido y empoderado frente a las responsabilidades de su equipo, por lo cual no interiorizan la responsabilidad por el accionar del personal a su cargo.

La Entidad cuenta con una evaluación 360 que permite evaluar el desempeño de cada colaborador. Además, se cuenta con un set de indicadores vinculados a los objetivos operativos y de cumplimiento por área, los cuales son evaluados a nivel de colaborador y revisados y monitoreados por la Gerencia de Auditoría Interna. Para el caso de Gerencias, la Gerencia General es la encargada de la revisión con cada uno de los responsables. Al respecto, se identificó que si bien se evalúan estos dos componentes, según la percepción de la Gerencia, no se cuenta con lineamientos y criterios que permitan evaluar el cumplimiento y nivel de adherencia a un adecuado Sistema de Control Interno.
No se han definido controles con respecto a posibles desviaciones del Código de Conducta y normas de la Entidad en la búsqueda del cumplimiento de los objetivos operativos y estratégicos por parte del personal.

4.2 Evaluación de Riesgo

P6: La Organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados
El análisis de este componente se centra no solo en identificar si la Entidad ha definido un inventario de riesgos, sino que si realiza la evaluación de estos a partir de objetivos definidos, y si estos son acordes con la realidad de la Entidad.

Si bien se han definido objetivos operacionales, así como iniciativas estratégicas y KPI´s para la aplicación y medición de los mismos, no se han definido formalmente las condiciones en las que se aceptará la modificación de los objetivos, tanto a nivel de alcance como de valores meta. Por otro lado, tampoco se encontró evidencia de la documentación de los objetivos iniciales de cada año a fin de validar que estos no fueron modificados en el transcurso de la gestión de la Entidad.

No se cuenta con lineamientos formalizados en los que se definan las acciones que serán requeridas para gestionar los riesgos no tolerables, es decir, aquellos que impactan en medidas no aceptables la consecución de los objetivos de la Entidad.
No se identificaron niveles de variación definidos como aceptables con respecto a las metas establecidas como objetivo, por tanto, no es posible identificar hasta qué punto se requerirá la toma de medidas correctivas, asignación de recursos adicionales o definición de planes mitigantes respecto al incumplimiento o cumplimiento parcial de alguna meta por objetivo.

No se ha definido el responsable para la identificación de cambios normativos externos que pudiesen afectar a los objetivos de la Entidad. Asimismo, se identificaron ciertas falencias con respecto a la

adecuación y cumplimiento total de las normativas de organismos reguladores aplicables. Con respecto a la precisión de la información, no se cuenta con políticas y procedimientos que permitan clasificar la información, y así, aplicar controles específicos al resguardo y custodia de información sensible. Con respecto a la difusión de información, no se ha definido el esquema para la comunicación de información frente a entes externos, que permita identificar aquella información que debe ser expuesta y difundida para propósitos que se alineen con los objetivos de la Entidad, como, por ejemplo, los logros obtenido en los últimos años.

P7: La Organización identifica los riesgos para la consecución de sus objetivos en todos sus niveles y los analiza como base sobre la cual determinar cómo se debe gestionar.
El análisis de este componente se centra en identificar si la Entidad cuenta con un proceso estandarizado para la evaluación de riesgos a todo nivel, de tal forma que le permita evaluar riesgos a nivel entidad y a nivel operativo.

Se identificó que, si bien es cierto que se realiza la evaluación de riesgos inherentes a nivel de proceso, para los procesos críticos seleccionados como parte del Plan Anual de Auditoría no se ha realizado el inventario total de riesgos operativos a nivel de procesos, por lo cual, podrían existir riesgos no tolerables que no están siendo evaluados ni monitoreados.
Con relación a los riesgos a nivel Entidad, se identificó que en el año 2015 se realizó la actualización de la calificación de los riesgos a nivel inherente con respecto a los resultados del 2014, sin embargo, no se identificó la actualización del alcance de los mismos, ni la adición o la eliminación sobre el inventario de riesgos frente a los cambios asumidos por la Entidad.
Las evaluaciones de riesgo son realizadas bajo criterio experto, ya que no se cuenta con historia sobre los eventos ocurridos para determinar con mayor exactitud los niveles de probabilidad o impacto sobre los riesgos inherentes.
La Entidad considera como tolerancia al riesgo, que todos aquellos riesgos que fueran superiores al nivel moderado deberían ser gestionados; sin embargo, no se encontró documentación formal en la que se definan las acciones a seguir y cómo o con qué tipo de control se deberán reducir, mitigar o controlar los riesgos, como parte de la gestión de riesgos de la Entidad.

P8: La Organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos
El análisis de este componente se centra en identificar que el marco teórico para la evaluación de riesgos tome en consideración los riesgos de fraude, y si se tiene en cuenta para cada objetivo a todo nivel. Si bien se ha definido un Código de Conducta, y el cumplimiento de este es monitoreado por el Comité de

Ética, parte del personal asegura no conocer este documento. Con respecto al monitoreo de posibles acciones fraudulentas por terceros, la Entidad no cuenta con procedimientos definidos que permitan definir controles a fin de monitorear el nivel de cumplimiento de las normas éticas por parte de proveedores, que en caso de incumplimiento podría afectar negativamente a la Entidad.

No se identificó como parte de los reportes presentados al Comité de Auditoría o Directorio, el resumen de aquellos hechos que podrían relacionarse con actividades fraudulentas, ya sea por informes elaborados erróneamente o con omisiones de forma premeditada, transacciones no recurrentes, actividades que vayan en contra de los controles definidos, transacciones realizadas que no tengan controles de segregación de funciones, entre otros. Con respecto a la posible elución de controles por parte de la Dirección, la Entidad no ha definido formalmente que toda acción o actividad que represente una excepción o desviación de control, como resultado de una decisión de la Gerencia o de algunas de las Gerencias, deba ser presentada a un ente revisor, como el Comité de Auditoría por ejemplo.

No se han identificado los objetivos operativos que pudiese incentivar acciones o medidas fraudulentas por parte del personal para el logro de los mismos, por tanto, si bien existen programas de compensación en los que se revisa el desempeño del personal, no se han identificado controles relacionados con la validación del otorgamiento de variables/incentivos para monitorear si el logro de los objetivos está soportado de alguna manera por acciones fraudulentas. La Entidad no cuenta con un control que permita distinguir los umbrales de cambios significativos en los aumentos de la compensación del personal.

Si bien se cuenta con una metodología de evaluación de riesgos, no se incluye como parte de la misma los siguientes aspectos:

- La definición de mecanismos que permitan la identificación y monitoreo de cuentas sensibles que podrían estar afectas a una mayor incidencia o probabilidad de eventos de fraude, como por ejemplo, las cuentas de inventarios, o los pagos variables de los incentivos por venta.
- La revisión periódica de aquellas transacciones realizadas bajo el esquema de "excepciones a los procedimientos", ejecutadas en plazos cortos que no permiten la revisión del alcance de las mismas por los entes superiores correspondientes.
- Revisión de esquemas automatizados, relacionados con posibles vulnerabilidades del sistema o ventanas para eludir los controles definidos.
- Revisión de entradas manuales versus posibilidad de registros automáticos.

P9: La organización identifica y evalúa los cambios que podrían afectar significativamente al Sistema de Control Interno

El análisis de este componente se centra en identificar si la Entidad cuenta con un proceso formal para evaluar los cambios significativos, internos y externos, que pudiesen surgir y materializarse a través de impactos negativos.

No se identificó actualización o modificación del alcance de los riesgos ya identificados; tampoco se observó la eliminación o la adición de nuevos riesgos emergentes en la realidad actual de la Entidad, en caso de aplicar, o sustento de que no se requieren cambios en los riesgos ya identificados. Asimismo, la Entidad no cuenta con procedimientos o un sistema de alertas que le permita identificar información que se relacione con la existencia o aparición de nuevos riesgos.

La Entidad implementó un nuevo sistema ERP, tanto para el *back* como para el *front office*, sin embargo, no se realizó una identificación formal de riesgos a nivel operativo a fin de cubrir con controles todos aquellos aspectos que hayan podido representar un riesgo.

4.3 Actividades de Control

P10: La Organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.

El análisis de este componente se centra en que las actividades de control o una combinación de control (como políticas, procedimientos y responsables) deben ser elegidas para reducir el riesgo de no alcanzar los objetivos a un nivel aceptable para la Entidad. Para esto, los controles deben ser evaluados en relación con los riegos que mitigan a nivel del proceso y de la Entidad.

Si bien se cuenta con una evaluación anual de los riesgos a nivel Entidad, se observa que los dueños de los procesos no se encuentran totalmente concientizados para asumir la responsabilidad de la correcta y oportuna ejecución de los controles. Por otro lado, observamos que la Entidad no ha identificado nuevos riesgos posteriores a la implementación de la plataforma informática, lo cual puede generar que las actividades de control no se encuentren orientadas a posibles riesgos calificados como críticos en el entorno actual.

La Entidad no cuenta con una cadena de valor formalmente definida, sin embargo, procede a realizar la evaluación de riesgos a través de un inventario de proceso por áreas y no por procesos transversales. Si bien, se ha realiza el inventario de riesgos y se ha vinculado con los objetivos estratégicos, no se han

definido riesgos orientados a objetivos de procesamiento de información como, por ejemplo: a) integridad con relación a la deficiencia de procesamiento de transacciones internas o con terceros, b) exactitud con relación al adecuado y oportuno registro en el procesamiento de información, c) validez con relación a corroborar la ejecución de eventos de acuerdo con los procedimiento definidos por la Entidad y d) tiempo de respuesta para la toma oportuna de decisiones. Es de suma importancia resaltar que la Entidad no ha documentado el análisis de segregación de funciones para cada uno de los procesos críticos o expuestos a riesgos. Tampoco ha analizado y documentado cada una de las actividades expuestas a error o fraude, a fin de asignarlas a distintos equipos de trabajo o personas. Los nuevos sistemas informáticos *People Soft* y *Campus Solution* no fueron parametados a la segregación de funciones necesaria.

En entrevistas realizadas, las Jefaturas tienen la percepción de que no se han definido, ni actualizado, ni difundido los procedimientos de aprobación y autorización para las actividades y tareas realizadas en los procesos de la Entidad.

P11: La organización define y desarrolla actividades de control a nivel de Entidad sobre la tecnología para apoyar la consecución de los objetivos.
El análisis de este componente se concentra en la tecnología como un elemento operativo clave de la Entidad, existiendo amenazas a los objetivos organizaciones a través del grado de madurez de la seguridad a nivel interno y externo. Es necesario que la Entidad identifique los controles generales y eficacia para mitigar riesgos importantes.

La Entidad no ha definido los controles de aplicación como parte de la evaluación de la confiabilidad de las tecnologías vigentes; es decir, los controles que permitan identificar el adecuado funcionamiento de los sistemas implementados y que mitiguen los riesgos implicados en el procesamiento de transacciones, por ejemplo: no cuenta con los activos, base de datos en relación con los cambios de programas y no se realiza un análisis de las principales incidencias respecto a las contraseñas, entre otros.

A la fecha, el departamento de TI no cuenta con una metodología para el aseguramiento de la calidad formalmente documentada de los servicios prestados a las áreas usuarias de la Entidad. Se incrementa la posibilidad de que no se cumpla con las fases y etapas definidas para propiciar tanto la detección de problemas oportunamente, el cumplimiento de los estándares de calidad, como así también los procedimientos y planes definidos por el mismo departamento. La Entidad no cuenta con documentación detallada de la arquitectura de TI para asegurar la solidez, integridad, escalabilidad y

flexibilidad de las nuevas tecnologías de solución e integración con las soluciones existentes (p.e. pistas de auditoría, tipo de aplicaciones, servicios, medios de respaldo de información, e interfaces) por lo cual no se cuenta con la posibilidad de, ante un incidente que afecte la integridad de la información, tener la trazabilidad histórica de lo sucedido. Tampoco se han identificado riesgos y controles a las amenaza externas en relación con el uso de la tecnología lo que lleva a una exposición de la información sensible de la Entidad (datos del alumnado, presupuestos por áreas, planillas, entre otros). No se ha realizado una revisión de los permisos de acceso, contrastándolos contra las políticas de otorgamiento de usuarios y perfiles con la finalidad de validar que estos sean correctos.

P12: La Organización despliega las actividades de control a través de políticas que establecen las líneas generales de control interno y los procedimientos que llevan dichas políticas a la práctica.
El análisis de este componente se centra en que las responsabilidades de las actividades de control deben ser identificadas y comunicados a través de políticas y procedimientos a todos los niveles de la Entidad.
Si bien la Entidad cuenta con documentos normativos internos (políticas y procedimientos, entre otros) que norman y establecen lineamientos para la ejecución de los procedimientos, existen algunos procesos para los cuales no se han emitido lineamientos. Lineamientos que reflejen la visión de la Alta Dirección sobre las actividades de control que se deberán llevar a cabo para el logro de los objetivos, respetando los niveles de tolerancia definidos por la Entidad. Adicionalmente, con la implementación de los nuevos sistemas informáticos *People Soft (Back Office) y Campus Solution (*Procesos *Core* del negocio*)* la documentación elaborada se encuentra desactualizada, pues no contempla las nuevas funciones que tiene el personal administrativo y docente. Los lineamientos emitidos para normar los procedimientos, así como la documentación de procesos con que cuenta la Entidad no indican lo siguiente: (a) dueño del proceso, (b) riesgos inherentes al proceso y controles existentes que ayuden a mitigarlos, y (c) Plantillas/matrices de evaluación de la segregación de funciones en cada proceso crítico.

La Entidad no ha elaborado el universo de controles a nivel proceso y por tal motivo, no se tiene definido formalmente la periodicidad en que se debe efectuar el 100% de los controles, lo cual incrementa el riesgo de que las evaluaciones no se realicen oportunamente y esto puede desencadenar la desnaturalización de aquellos controles preventivos, convirtiéndolos en solo detectivos. Respecto a las medidas correctivas (planes de acción) no se ha definido formalmente cuántas veces se puede modificar la fecha de implementación de un plan de acción y quién será el funcionario responsable de aprobar dicho cambio; tampoco se ha establecido si los dueños de los procesos involucrados deban definir controles mitigantes en caso de replantear dicho plan.

El área de Auditoría Interna es la responsable de realizar el seguimiento a los planes de acción para la implementación oportuna; sin embargo, entre los integrantes observamos que ninguno cuenta con alguna certificación internacional que respalde el conocimiento, las habilidades y las destrezas del auditor interno para la práctica de la actividad de auditoría interna.

4.4 Información y Comunicación

P13: La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.
El análisis de este principio se enfoca en que la información pertinente, oportuna y de calidad debe ser evaluada por la Alta Dirección y otros para ayudar a abordar e identificar: (a) las características de la información de calidad y (b) que la información se adapte a las necesidades de las gerencias.

Si bien la Entidad cuenta con información que es analizada y evaluada para la toma de decisiones como son: 1. Plan Estratégico, 2. Plan Táctico, 3. Presupuestos y 4. Estados Financieros, sin embargo, no ha identificado cuál es la información clave requerida para que los procesos operen y cuál es la información que generan los mismos. Asimismo, no se ha identificado cuáles son los niveles de responsabilidad en relación con la elaboración y aprobación de la información que se genera dentro de cada proceso. Por otro lado, no se ha evaluado la confiabilidad de los sistemas informáticos a fin de conocer la pertinencia de la información que se obtiene a partir de ellos para propósitos de análisis, presentación de resultado y comunicación a la Alta Dirección.

En cuanto al tratamiento de fuentes de datos externas la Entidad principalmente trabaja con las normas emitidas por el Ministerio de Trabajo y el Ministerio de Educación; sin embargo, no cuenta con una política o procedimientos de control de cambios normativos así como el nombramiento de un responsable para el monitoreo y evaluación del cumplimiento normativo.

La Entidad no ha definido los niveles de revisión de la información que se genera dentro de cada proceso. Así como tampoco cuenta con una política de gestión, calidad y gobierno de información que establezca la obligación de los miembros de la Entidad de verificar que la información que ellos generan y los datos que se exponen ante un tercero (interno o externo) estén de acuerdo con la realidad. Tampoco se ha definido una política sobre la gestión física de los datos, almacenamiento y nivel de seguridad, así como no se han identificado los niveles de accesos a los empleados según el nivel de criticidad de la información. Así mismo, no se ha evaluado el costo beneficio respecto a la naturaleza, cantidad y precisión de la información. La Entidad ha optado por no activar los log de información a

partir de la implementación del nuevo ERP (*People Soft*); sin embargo esta decisión no cuenta con el soporte de un análisis de costo beneficio respecto a la información que pudiese obtener, a la capacidad requerida en cuanto al volumen de datos que se debe mantener y tampoco se ha considerado el impacto negativo respecto a la modificación o pérdida de información sensible.

P14: La Organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del Sistema de Control Interno.
El análisis de este principio se centra en que la información que se comunica internamente es importante y se debe comunicar a las personas con responsabilidades sobre los objetivos de operación, de cumplimiento y de información.

La Entidad no cuenta con un procedimiento formal para comunicar a todo el personal respecto al control interno, los objetivos, importancia, relevancia y beneficios de tener un adecuado Sistema de Control Interno. Por otro lado, en los procesos cuyas actividades se encuentran documentadas no se define claramente cuáles son las personas encargadas de ejecutar los controles en los procesos. Tampoco se ha definido qué información se publicará respecto a las desviaciones de control identificadas. El "Canal de Gestión Ética", herramienta que sirve para comunicar anónimamente cualquier preocupación seria y sensible relacionada con potenciales irregularidades e incumplimientos del Código de Conducta, no se encuentra habilitado para el uso de los proveedores y del alumnado en las sedes de provincias.

Si bien se cuenta con ciertos mecanismos de comunicación tanto interna como externa (*Mailing*, portal Web y reuniones informativas), no se ha establecido una política que establezca los medios de comunicación internos y externos más favorables en términos de estandarización y efectividad.

P15: La organización comunica a las partes externas interesadas los aspectos clave que afectan al funcionamiento del control interno.
El análisis de este principio se centra en que la comunicación externa no se limita a los informes sobre el control interno o sobre la información financiera. También se reconoce que las partes externas pueden proporcionar información a la Alta Dirección sobre la efectividad del control interno.

La Alta Dirección no ha definido formalmente (en un documento) los diversos métodos de comunicación que maneja y según el público objetivo, el tipo de comunicación, tiempo de respuesta y requisitos legales o regulatorios. Se observa que la Entidad cuenta con diversos métodos de comunicación como portal Web, correo electrónico del personal administrativo, docente y alumnado,

redes sociales y, en caso fuere necesario, notas de prensa a nivel entidad o a nivel agremiación (Asiste Perú).

El resultado de las evaluaciones realizadas por un consultor externo es expuesto al Directorio siempre y cuando se tome en cuenta la importancia del objetivo de la consultoría, criticidad del proceso evaluado así como el costo de la contratación. Sin embargo, estos criterios no se han definido formalmente en políticas y procedimientos tanto para la Alta Dirección como para el Directorio. Como se indicó en el principio 14, el "Canal de Gestión Ética" no se encuentra contemplado para el uso de los proveedores y al alumnado en las sedes de provincia.

4.5 Actividades de Supervisión

P17: La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la Alta Dirección y el Directorio, según corresponda.

El análisis de este principio se enfoca en las deficiencias detectadas, si son informadas oportunamente a los responsables (Dueño del proceso, Alta Dirección y el Directorio) para la adopción de medidas correctivas oportunamente. La Entidad no ha definido formalmente actividades de supervisión relacionadas con las evaluaciones continuas de las actividades de gestión y supervisión diaria de los empleados con el objetivo de obtener información en tiempo real e identificar deficiencias con mayor rapidez.

Capítulo V. Diseño de los planes de acción propuestos para la implementación y levantamiento de brechas en relación con un sistema de control interno fortalecido.

El Marco COSO (2013) no determina específicamente los controles que se deben definir, seleccionar, desarrollar o implementar para que su Sistema de Control Interno sea determinado como efectivo. La determinación de estos está condicionada al criterio experto en función de los factores específicos de cada organización, tales como:

- Las leyes, reglas, regulaciones y normas aplicables a la organización.
- La naturaleza del negocio de la Entidad, así como la de los mercados en que opera.
- El alcance y la naturaleza del modelo operativo adoptado por la Dirección.
- La capacidad del personal responsable del control interno.
- El uso y la dependencia de las tecnologías.
- Las respuestas adoptadas por la Dirección ante los riesgos evaluados.

En cuanto a las especificaciones del Marco seleccionado en el presente trabajo de investigación, teniendo en cuenta los resultados del Diagnóstico realizado acerca de la situación actual de la Entidad en relación con el Sistema de Control Interno sobre los lineamientos definidos por el Marco COSO 2013, y con el propósito de minimizar las brechas del cumplimiento de los principios relevantes, se han definido planes de acción que permitan a la Entidad acortar las brechas con respecto al cumplimiento efectivo de los componentes del Marco.

Cabe señalar que la definición de los planes de acción se ha limitado a aquellas actividades que presentan una mayor deficiencia de control de los componentes evaluados en cuanto a presencia y funcionamiento, y tomando en consideración la opinión de la Dirección de la Entidad sobre el rumbo a seguir para la gestión del control interno en la Entidad.

1.- Actualización de procedimientos considerando lo indicado en el COSO 2013

Debido a la implementación de nuevos sistemas informáticos (*Peoplesoft y Campus Solution*) y considerando el desarrollo del análisis de segregación de funciones, la Entidad debe actualizar la documentación de los procedimientos considerando lo siguiente:

- Dueño del proceso
- Riesgos inherentes al proceso y controles existentes que ayuden a mitigarlos.
- Plantillas/matrices de evaluación de la segregación de funciones en cada proceso crítico.

Asimismo, esta actividad facilitará identificar los procesos claves que no cuentan con procedimientos y controles formales. Conforme se realice la actualización de documentación, se avanzará con el inventario de controles implementados dentro de la organización en todos los niveles. Esta información será de gran ayuda al área de Auditoría Interna como *input* para la elaboración del Plan de Auditoría Anual a fin de conocer el alcance de los controles a evaluar respecto a eficiencia y eficacia, y determinar la periodicidad para evaluar el total de estos.

2. Actualizar y formalizar políticas y procedimiento de TI

La Entidad debe ejercer actividades de control general de TI abarcando todos los sistemas de aplicación para garantizar la integridad, confiabilidad y precisión de los mismos. Por tal motivo, es necesario actualizar y formalizar, según sea el caso, las políticas y procedimientos de TI considerando los siguientes temas:

- Normas de desarrollo de sistemas
- Políticas y procedimientos de seguridad de la información
- Normas de recuperación y respaldo
- Acuerdos de nivel de servicios con proveedores
- Procedimientos y prácticas de monitoreo de redes
- Normas sobre codificación de programas
- Normas sobre los productos y arquitectura de *hardware*
- Normas sobre instalación, configuración y pruebas de *hardware y software*

Esta acción supone que las actividades de control se encuentren en el nivel superior y no se realicen de forma individual por aplicación adquirida. Al centralizar las actividades de control se generará un enfoque con mayor consistencia, confiabilidad y control para todos los sistemas de información en la Entidad. El Instituto de Auditores Internos (2006) nos indica las tres áreas más importantes para las actividades de control general que son:

- Seguridad física y de la información
- Gestión del cambio
- Continuidad del negocio y recuperación de desastres

Asimismo, es importante que la Entidad deba redefinir la estructura organizacional del área de TI, estableciendo puestos correctamente segregados y conforme a una evaluación de la capacidad para la atención de servicios de TI y establecer un catálogo de servicios de TI que brindará el área a partir del establecimiento de la nueva estructura organizacional y los nuevos procedimientos, considerando que este catálogo deberá ser formalizado y difundido a las demás áreas de la Entidad.

3.- Elaboración de políticas y reglamentos requeridos por la Entidad para fijar las reglas de conducta

La adopción de políticas y reglamentos tiene como objetivo fijar las reglas de conducta de la Entidad, definir a los responsables directos de lograr los objetivos y detallar las obligaciones y los procedimientos que deben cumplir los directores, funcionarios, empleados y asesores que manejan información privilegiada. Por tal motivo, se ha visto por conveniente el formalizar las políticas y procedimientos de la Entidad, para ello es recomendable:

- Elaborar un inventario de las políticas y reglamentos requeridos por la Entidad: el Directorio y la Alta Dirección deben elaborar un inventario de políticas y procedimientos que contenga un listado detallado de todas las políticas y reglamentos que la Entidad requiere para la eficiente ejecución de las operaciones y para dar soporte al Código de Ética. Adicionalmente, se debe indicar el estado del documento (Existente, inexistente o en proceso de elaboración), el propósito de cada política, los objetivos que busca alcanzar, y las áreas de la Entidad que se verán afectadas por su aplicación.
- Definir responsables y fechas para la elaboración y actualización de las políticas y reglamentos: del inventario elaborado se debe asignar formalmente a los responsables de elaborar y actualizar estos documentos. De manera adicional, se deben definir los plazos para la elaboración de las políticas y reglamentos, así como la periodicidad en que será revisada y actualizada la documentación.
- Elaborar las políticas y reglamentos: las políticas y reglamentos deberán ser elaborados tomando en consideración una estructura y un formato estandarizado el cual refleje homogeneidad en la Entidad. De manera general, todas las políticas y reglamentos deberán especificar su propósito y objetivos, y su cuerpo deberá contar con un nivel de detalle que haga evidente este propósito y que permita identificar fácilmente los derechos, obligaciones y responsabilidades de aquellos cargos sujetos a cada política o reglamento, evitando ambigüedades. Finalmente, se podrá incluir un glosario de términos, en caso se esté utilizando lenguaje o terminología técnica.
- Someter las políticas y reglamentos a la aprobación del Directorio: las políticas y procedimientos deben ser presentados en la sesión de Directorio más cercana y sometida a aprobación. La aprobación del Directorio debe ser registrada mediante la firma de sus miembros en el documento original, el cual será posteriormente digitalizado y difundido.
- Difundir y comunicar la implementación de las políticas y reglamentos: el éxito en la aplicación de las políticas y reglamentos dependerá en gran medida de una adecuada comunicación y difusión. Por tal motivo, es necesario preparar estrategias de comunicación que involucren a las partes interesadas (Directorio, Alta Gerencia, gerencias de líneas, empleados, entre otros) por ejemplo, talleres de sensibilización o capacitación. Adicionalmente, estos documentos deben ser difundidos por medios que sean accesibles a todos aquellos que estén sujetos a ellos.

4.- Elaboración de una política de presentación y revelación de la información

La Entidad debe definir los lineamientos, aplicables a todos los colaboradores de la organización, sobre el trato que debe ser dado a la información interna y el proceso al que esta debe ser sometida antes de su revelación a los grupos de interés. Dichos lineamientos deberán ser formalizados en una política que deberá contener, al menos, las siguientes secciones:

- Clasificación, revelación y divulgación de la información
- Acuerdos de confidencialidad
- Medidas para la protección de la información confidencial
- Uso de página Web y medios electrónicos
- Lineamientos para los boletines o comunicados de prensa

La política deberá ser sometida a la aprobación del Directorio y, una vez aprobada, deberá elaborarse una estrategia para su divulgación interna. Respecto a la protección de la información confidencial, EY Perú (2014) indica que es necesario que la Entidad elabore un marco de clasificación de datos que permita a los colaboradores identificar, etiquetar y proteger los datos sensibles, considerando lo siguiente:

- Una política de clasificación de datos, que defina el alcance, las responsabilidades y otros requerimientos de gobierno dentro de una organización, para manejar eficazmente la implementación de diversos niveles de protección de datos para diferentes tipos de información.
- Un esquema de clasificación de datos, que determine los estratos de datos y los niveles de protección asociados, y que describa cada nivel.
- Lineamientos de etiquetado de datos, con instrucciones para etiquetar la información de una forma que permita a los usuarios determinar visualmente con facilidad el nivel de clasificación de un documento.
- Lineamientos de manejo de datos, que proporcionen requerimientos específicos para proteger los datos de acuerdo con su nivel de clasificación y definiendo cómo se deben almacenar, transmitir y procesar los datos de cada nivel.
- Mapa de clasificación de datos a ser utilizados por los dueños de los datos para vincular conjuntos de datos o tipos de datos con los niveles de clasificación, considerando qué datos son sensibles y útiles, tanto para los equipos de soporte (protección de datos) y para los usuarios finales.

5.- Elaboración de políticas y procedimientos de control de cambios normativos

La Entidad debe determinar la forma más apropiada y eficiente de implementar el monitoreo y evaluación del cumplimiento normativo de acuerdo con sus propias necesidades y organización interna;

por lo cual, es necesario el nombramiento de un responsable para la ejecución de dicha labor. Las principales responsabilidades que debe contemplar dicha labor son:

- Asesoramiento a la Alta Dirección sobre el cumplimiento de la normativa aplicable a la Entidad.
- Informar oportunamente a la Alta Dirección los principales cambios en la normatividad que pueda producir un impacto en las operaciones de la Entidad.
- Vigilar el cumplimiento normativo de la Entidad
- Informar periódicamente a la Alta Dirección el progreso de la implementación de las nuevas normativas o cambios de las mismas. Así como proponer medidas correctivas en caso de presentar retrasos en la correcta aplicación.
- Orientar al personal de la Entidad sobre la importancia del cumplimiento normativa y el impacto que podría ocasionar el incumplimiento respectivo.
- Otras funciones que la Alta Dirección considere adecuadas.

La política y los procedimientos referidos al Cumplimiento Normativo, en los que se establezca formalmente las funciones mencionadas anteriormente deben ser aprobados por la Alta Dirección. Asimismo, dicho documento debe contener las principales pautas para prevenir, identificar y mitigar el incumplimiento normativo en todos los niveles de la organización.

6.- Definir y formalizar medidas de control para el monitoreo de los objetivos

A fin de que exista una adecuada evaluación de lo ejecutado versus lo planificado, se recomienda que los objetivos definidos por la Entidad y aprobados por el Comité de Gerencia y el Directorio, así como las estrategias y metas esperadas se encuentren documentados formalmente en las Actas del Directorio y sean custodiados como un documento base por el área de Auditoría Interna. Se recomienda también que se defina a qué nivel de detalle estos deben ser conocidos por el personal, considerando el nivel de confianza de estos, así como el nivel de repercusión que tendrá el conocimiento de ciertas metas operativas en el desempeño positivo o negativo del personal.

Para la oportuna toma de decisiones con respecto al cumplimiento de los objetivos, se debe contar con información oportuna y certera, por ello, es importante considerar el monitoreo de los resultados reportados por el personal en relación con las metas por objetivos operacionales, estableciendo frecuencias y niveles de revisión. Sin embargo, es importante considerar también que ciertos resultados deberán ser validados, por lo cual, se debe definir qué información a nivel de reportes o informes, así como las fuentes que deberán ser consultadas para validar los resultados de las metas por objetivos operacionales reportadas por el personal. Esto permitirá que, en caso de ser necesario, algunos recursos

puedan ser reasignados de manera eficiente y que se realicen comparaciones evolutivas, es decir, con resultados de indicadores en años pasados.

En caso de requerir modificaciones a los valores meta de los objetivos operacionales que excedan la tolerancia definida, se debe especificar cuáles serán los niveles de revisión y aprobación, así como el análisis del impacto que tendrá dicha modificación en otros objetivos o en los objetivos estratégicos. Se recomienda que la revisión requerida pase por los mismos niveles que se establecieron para la aprobación de los objetivos.

7.- Consolidar las políticas de evaluación de riesgos para todos los niveles de la organización

La identificación y evaluación de riesgos es un proceso que permite a la Entidad ampliar la probabilidad del logro de los objetivos, ya que, al conocer los mismos y al haber identificado el nivel en que estos podrían afectar la consecución de los objetivos, la Entidad podrá adoptar las medidas necesarias para el tratamiento del riesgo y así, se vea menos afectada frente a la posible materialización de este.

Se recomienda a la Entidad definir y formalizar una metodología para la evaluación de riesgos, que considere a mediano plazo no solo la evaluación y control, sino también la gestión de los mismos, lo que representa una metodología más fortalecida, orientada a la correcta y adecuada asignación de esfuerzos en función de los riesgos que está dispuesta a afrontar la Compañía. Con base en el análisis de la metodología recomendada por la consultora Ernst & Young (2014) y de COSO (2013), los temas que se consideran relevantes para ser incluidos en la metodología de evaluación de riesgos son los siguientes:

Identificar la cadena de valor, entendiendo por este concepto la estructura que organiza los procesos de la Entidad y permite, a su vez, ofrecer una propuesta de valor para los *stakeholders*. El objetivo de contar con la cadena de valor permitirá a la Entidad delimitar aquellos procesos que como parte del negocio debe identificar, así como los subprocesos, responsables, actividades, y entradas y salidas por cada componente.

Para la esquematización de la cadena de valor se debe tener en cuenta que la misma estará conformada por tres tipos de procesos:

- Estratégicos: que estarán relacionados con la estructura, organización, lineamientos y directrices gerenciales y de administración de la Alta Dirección.
- De Negocios: enfocados en la parte operativa y son aquellos que dan soporte a la ejecución de políticas y estrategias relacionadas a los *stakeholders.*
- De Soporte: son aquellos que tienen por función dar soporte a los procesos anteriores.

Identificar los factores de riesgo que pudiesen afectar a la Entidad: de acuerdo con el Marco COSO (2013), se recomienda a la Entidad incorporar, como parte de sus procedimientos para la identificación y evaluación de riesgos, las siguientes fuentes de riesgo externas e internas:

- Económicos: en función de aspectos que podrían afectar el capital y el financiamiento.
- Entorno natural: catástrofes o cambios ambientales causados por el hombre o la naturaleza, que podrían afectar negativamente a la Entidad, ya sea por pérdidas de información o de capacidad para operar.
- Regulatorio: referido a cambios regulatorios que podrían representar nuevas exigencias para la Entidad.
- Sociales: en relación con los cambios en las necesidades y expectativas del cliente.
- Tecnología: avances y nuevas tecnologías que podrían representar una ventaja o desventaja en caso de no contar con las mismas. Así como las medidas de control a fin de afrontar interrupciones de sistemas para continuar con la operatividad de la Entidad.
- Infraestructura: en relación con los recursos que puedan afectar la disponibilidad de las infraestructuras.
- Estructura de la Dirección: cambios organizativos que pudieran afectar la base de la visión de control interno de la Gerencia.
- Personal: en relación con la predisposición del mismo a aceptar la visión de control interno propuesta por la Gerencia.
- Accesos a Activos: en relación con el acceso de los activos y las medidas de protección establecidas para evitar la apropiación ilícita de los mismos.

En adición, la Entidad debe considerar como factor relevante en la identificación todos aquellos cambios afrontados por la Entidad por nuevas decisiones de negocio, crecimiento y nuevas tecnologías, entre otros; para así, incluir como parte de los riesgos identificados aquellos riesgos emergentes que pudiesen afectar la evaluación. Es importante considerar también los riesgos que se originan a partir de las acciones de terceros, es decir proveedores de bienes y servicios externos.

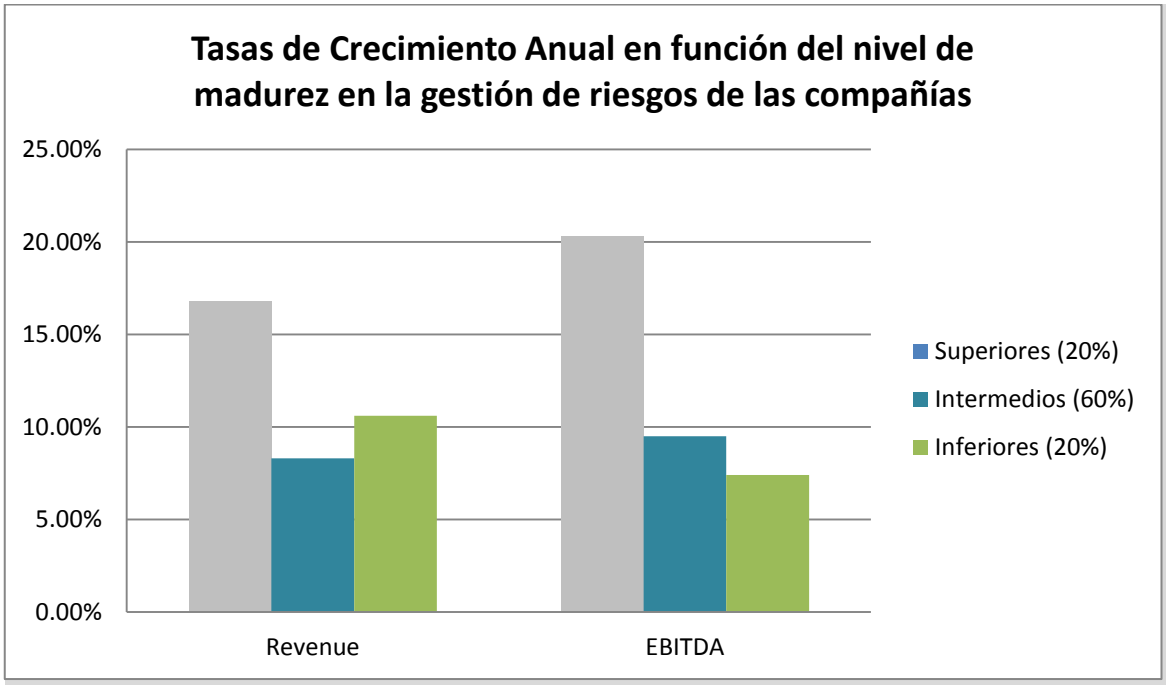
Definir riesgos en todos los niveles de la Entidad, así como en sus unidades operativas: de acuerdo con lo interpretado sobre la base del Marco COSO (2013), y el enfoque de auditoría basada en riesgos, propuesta en el Reglamento de Auditoría Interna de la SBS (2008) la gestión de riesgos implica evaluar los riesgos a dos niveles: (a) a nivel entidad y (b) a nivel de transacciones, es decir, a nivel operativo por proceso. Esta última consideración permite a la Entidad mantener niveles aceptables y con cierta

homogeneidad a nivel de organización, contribuyendo a la consecución de los objetivos operativos, y así en cadena a la consecución de los objetivos estratégicos

8.- Realizar la identificación y análisis de riesgos

De acuerdo con la publicación de EY, "Convirtiendo riesgos en resultados" (2013). En consideración de las más recientes crisis financieras, la visión de los altos ejecutivos ha cambiado respecto de la gestión de riesgos. De acuerdo con lo indicado por la consultora, sobre la base de los estudios e investigaciones realizadas, las empresas con una gestión de riesgos más madura generalmente superan a sus pares financieramente, lo cual repercute en el mayor crecimiento a nivel de ingresos y EBITDA, tal como se puede apreciar en el gráfico 1.

Gráfico 4. Crecimiento anual en relación con la madurez en la gestión de riesgos



Fuente: EY Global, Turning risk into results, 2013

En relación con el creciente interés en la gestión de riesgos y la mayor importancia otorgada por los líderes de empresas en crecimiento, se sugiere a la Entidad fortalecer la metodología para la identificación, evaluación y tratamiento de los riesgos. La metodología para la evaluación de riesgos puede variar de acuerdo con cada Entidad, sin embargo, se recomienda que esta incluya la evaluación de la probabilidad de ocurrencia y del impacto.

De acuerdo con lo analizado a partir del Marco COSO (2013), se entiende por probabilidad la posibilidad de que ocurra un evento determinado; el impacto representa el efecto de esta posibilidad. La probabilidad puede ser medida en función de la cantidad de eventos, a la complejidad del proceso, entre otros escenarios. El impacto en cambio, puede ser medido en función del patrimonio, de las ventas, de la reputación, de la interrupción, de las multas, etc.
Otros parámetros considerados para una evaluación de riesgos alternativa y más desarrollada incluye: (a) la evaluación de la velocidad en que pueda ocurrir el impacto y (b) la duración de tiempo del impacto una vez que el riesgo se haya materializado.

La consideración de información basada en experiencia interna, sobre hechos ocurridos y riesgos materializados, así como la experiencia sobre el sector de la Entidad, permitirá también un análisis mucho más certero sobre los criterios de probabilidad e impacto a ser considerados para cada riesgo.
Es importante también considerar el horizonte de tiempo en que estos riesgos son medidos. Es recomendable que el horizonte sea concordante con el esperado para el cumplimiento de los objetivos estratégicos. Otro aspecto importante para la evaluación de riesgos es la distinción entre riesgo inherente y riesgo residual:

- Riesgo inherente: es el riesgo en su forma natural, sin considerar la existencia ni la aplicación de controles.
- Riesgo residual: es el riesgo resultado de la aplicación de un mitigante, es decir, de un control existente que modifica el nivel en que este riesgo puede impactar en caso sea materializado o cómo puede disminuir la probabilidad de ocurrencia.

La combinación para la evaluación de riesgos considera la evaluación del impacto y la probabilidad, la cual puede tomar los niveles que la Entidad considere pertinentes. Para el propósito del presente trabajo de investigación y sobre la base de la experiencia y el conocimiento de la Entidad, se recomienda que se consideren 4 niveles: Extremo, Alto, Moderado y Bajo.
Cada uno de los riesgos identificados deberá ser evaluado en función de estos 4 niveles para los criterios de probabilidad e impacto.

De acuerdo con lo indicado en la metodología de riesgos de la consultora Ernst & Young (2014), <<Para calificar la “Probabilidad” e “Impacto”, se debe seleccionar el criterio general respectivo más idóneo según las características del riesgo. En caso el riesgo esté relacionado con más de un criterio general, se deberá seleccionar el que esté intrínsecamente más relacionado con el riesgo o el criterio en el que se logre mayor calificación. Las calificaciones que se obtengan por cada riesgo deberán ser

documentadas en la matriz de Riesgos y Controles >>. El resultado de esta evaluación se conocerá como riesgo inherente o riesgo residual.

9.- Realizar la identificación y calificación de controles

Para la identificación de controles, definida la calificación de cada riesgo a nivel inherente, se identifican los controles asociados a cada riesgo. Se entiende como control a toda aquella medida que mitiga en alguna forma el riesgo, ya sea disminuyendo la probabilidad de ocurrencia, o de lo contrario, disminuyendo el impacto. De acuerdo con la metodología de riesgos de la consultora Ernst & Young (2014), para la documentación de controles, se debe tener en cuenta responder a las siguientes preguntas:

- ¿Qué busca hacer el control? detallando actividades claramente definidas
- ¿Cómo se lleva a cabo el control? detallando cómo es que el control mitiga el riesgo
- ¿Quién lleva a cabo el control? para lo cual se espera que se haya definido un responsable
- ¿Cuándo se realiza el control? detallando frecuencia definida o idónea de acuerdo con las características del riesgo
- ¿Se encuentra documentado el control? el control debe dejar, además, evidencia de su existencia y desarrollo
- ¿Existe una adecuada segregación de funciones?

Identificados los controles, se deberán documentar también en la matriz de riesgos y controles, teniendo en consideración para la evaluación dos aspectos: (a) diseño del control y (b) operatividad o ejecución del control. Para el diseño se evaluará la definición del control, es decir, si tal cual ha sido diseñado realmente logra atacar en alguna medida la probabilidad o impacto del riesgo al que aplica. Para que un control se encuentre correctamente diseñado debe responder a las preguntas indicadas en el párrafo anterior.

La calificación de los controles puede obedecer a diferentes niveles de fortaleza en función de diseño y ejecución. Para propósitos del trabajo de investigación, se propone que estos sean mapeados en: Débil, moderado y fuerte.

Calificados los controles en relación con el diseño y operatividad, se deberá considerar la calificación a nivel ponderado en función de todos los controles aplicables a un mismo riesgo, y así definir en qué medida la existencia y ejecución del control afecta al riesgo, para así obtener la calificación del riesgo residual.

10.- Definir y delimitar las acciones requeridas para los niveles de apetito y tolerancia

Uno de los componentes más importantes para gestionar los riesgos es la identificación del apetito por el riesgo, entendiendo por este concepto el nivel de riesgo que la Entidad está dispuesta a asumir en la búsqueda de sus objetivos estratégicos. El apetito por el riesgo se engloba a través de políticas, lineamientos, directrices y procedimientos y deber ser evaluado y analizado en función del crecimiento de la compañía y los objetivos de retorno financiero. Por otro lado, la definición y comprensión de los niveles de tolerancia, entendida como el nivel de riesgo que la Gerencia está dispuesta a aceptar en la variación de sus objetivos estratégicos, permiten a la Entidad tener la capacidad de convivir a la par con los riesgos, teniendo la capacidad de operar y gestionar dentro de dichos niveles de riesgo.

El discutir y definir un nivel de tolerancia a nivel de organización incrementa la probabilidad de que la organización pueda lograr sus objetivos. La tolerancia deberá ser más rígida con respecto a la evaluación de riesgos relacionados con cuestiones de cumplimiento. Para optimizar los recursos en función de la definición de controles, monitoreo y seguimiento de planes de acción, que implica la asignación de recursos a dichas actividades, se recomienda considerar y evaluar la aplicación de dichas actividades en función de los niveles de tolerancia.

De acuerdo con lo recomendado por la consultora Ernst & Young en su metodología de gestión integral de riesgos (2014) se indica que como parte de los procedimientos a tener en cuenta para la actualización de los límites de apetito y tolerancia se debe considerar:

- Revisión en el primer trimestre del año de los límites con los gerentes de cada área y la Gerencia General. El establecer el apetito por el riesgo y la tolerancia es cuestión que implica a los altos mandos, ya que la determinación de la misma debe soportarse en el análisis del tipo de industria, así como de los eventos históricos que hayan afectado a la empresa en su crecimiento.
- Definir quién cumplirá el rol de facilitador en los talleres para la actualización de límites.
- Determinación de los niveles de apetito y tolerancia: La Gerencia deberá definir los niveles que está dispuesta a aceptar y gestionar en función de los objetivos y el plan estratégico trazado. Además, se recomienda evaluar los recursos asignados en años anteriores para gestionar los riesgos.
- Documentación de acuerdos: se deberá preparar un acta con los acuerdos, la cual será presentada en Comité de Directorio/ Comité de Riesgo.
- De acuerdo con lo indicado en el Marco COSO (2013), evaluado el riesgo a nivel de probabilidad de ocurrencia e impacto, la Entidad deberá definir el cómo debe gestionar en función del nivel de apetito y tolerancia al riesgo definido, para ello se recomienda considerar:
- Respuesta al riesgo

En función del análisis de las respuestas al riesgo propuestas por el Marco COSO, se recomienda a la Entidad tomar en cuenta lo siguiente:

- Explotar: aceptar niveles altos de riesgo para así aprovechar oportunidades
- Aceptar: conservar el riesgos sin implementar medida alguna
- Evitar: para lo cual se deja de realizar la actividad que origina el riesgo
- Reducir: establecer controles que pueden reducir la probabilidad, el impacto o ambas a la vez,
- Compartir: se toman medidas que permiten a la organización reducir la probabilidad, el impacto o ambos transfiriendo de alguna forma el riesgo o parte de él.

- Revisión iterativa del riesgo en función de la tolerancia

  Todas las respuesta al riesgo a ser implementadas no disminuirán en forma considerable los niveles de probabilidad o impacto, sin embargo, siempre y cuando sigan superando los niveles de tolerancia aceptados por la Entidad, la Gerencia deberá realizar nuevamente la respuesta al riesgo

- Análisis de costo beneficio

  Se recomienda considerar todas las opciones para dar respuesta al riesgo identificado, y en función de ellas realizar un análisis y cuantificación de los posibles costos implicados en la implementación de la acción para el tratamiento del riesgo, ya que se entiende que una Entidad no tiene recursos ilimitados, por lo que deberá enfocar sus esfuerzos en aquellas actividades que le proporcionen un mayor beneficio, es decir, una mayor reducción del riesgo con el menor costo. Se deberá evaluar cuál es el efecto que tiene el tratamiento, y si este mitiga la probabilidad o el impacto.

- Considerar procedimientos existentes

  Se recomienda antes de implementar o definir una actividad nueva para dar respuesta al riesgo, tomar en consideración los procedimientos y controles implementados y evaluar si estos pueden ser modificados a fin de dar la respuesta al riesgo requerido y de mejor gestión.

  De acuerdo con lo definido en el Marco COSO, «el control interno no incluye asegurarse de que se adopta la respuesta más óptima para abordar los riesgos identificados» (COSO 2013:97), aspecto que sí es considerado por la gestión de riesgos, por lo cual se recomienda a la Entidad tomar en consideración ambos marcos de gestión para dar una respuesta al riesgo que permita a largo plazo definir una base para la gestión integral de riesgos.

- Segregación de funciones

  A fin de que la respuesta al riesgo permita la reducción al riesgo esperada teniendo en consideración los niveles de segregación requeridos para un adecuado funcionamiento y prevención con respecto a acciones fraudulentas.

11.- Elaboración del "Plan de sucesión de puestos claves"

Con la finalidad de evitar que no se alcancen los objetivos de la Entidad debido a que un puesto clave de la organización quedó de forma temporal o permanente vacante se debe elaborar un "Plan de sucesión de puestos claves". El IFC (2010) indica que la planificación de la sucesión debe ser parte integral de la política general de gestión del personal, siendo este un tema importante y estratégico para la Entidad, por lo que el Directorio debería supervisarlo. Una óptima planeación ofrece las siguientes ventajas:

- Ofrece a los promotores una expectativa confiable de la continuidad del negocio.
- Sirve como ejemplo a la gestión de personal de toda la empresa y puede ser un modelo para la planificación del desarrollo profesional dentro de la misma.
- Motiva a los gerentes de nivel medio, mediante actividades de desarrollo y reconocimiento.

Es necesario que los planes de acción a diseñar consideren los siguientes puntos:

- Planes de sucesión de emergencia para el Director Ejecutivo, la Alta Gerencia y otros puestos claves de la organización.
- Sistema de evaluación de las competencias y las habilidades necesarias para cualquier puesto.
- Programa para el desarrollo profesional del personal.
- Sistema para facilitar la búsqueda, fuera de la organización, de posibles candidatos a puestos clave.

12.- Administración de Riesgo de TI

De acuerdo con el Marco COSO (2013) actualmente la tecnología representa un esencial soporte para el logro de los objetivos ya que ha permitido mejorar y en algunos casos automatizar los controles sobre las actividades de una organización; sin embargo, la innovación tecnológica presenta a la vez un incremento en la complejidad de ciertas operaciones, lo que en caso no se cuente con una adecuada administración de riesgos, podría significar mayor dificultad en la identificación y gestión de los mismos.

El entorno tecnológico requerido se deberá adecuar a la magnitud de cada Entidad. Al respecto, si bien el entorno tecnológico dependerá de la magnitud de cada Entidad, se recomienda definir y establecer una matriz de riesgos de Tecnología de la Información, en la que se indiquen los niveles de probabilidad, impacto, riesgo inherente, residual, controles establecidos, responsable, periodicidad y evidencia de sustento. De acuerdo con las publicaciones de EY México (2012) se sugiere un universo de 10 categorías de riesgo:

- Legal y reglamentario
- Proveedores terceros y *outsourcing*
- Administración de programas y del cambio
- Seguridad y privacidad
- Entorno físico

- Dotación de personal
- Operaciones
- Datos
- Infraestructura
- Aplicaciones y bases de datos

Adicionalmente, nos menciona que las empresas deben diseñar metodologías y procedimientos para la evaluación periódica de los riesgos definidos. Es de suma importancia mantener actualizados los procesos y procedimientos operativos y, a su vez, relacionados directamente con los riesgos administrados. Para esto es necesario considerar lo siguiente:

- Un análisis de escenarios para desastres y eventos.
- Administración de pérdidas por incidentes para registrar los eventos y estimar su impacto financiero.
- Aseguramiento y coordinación reglamentaria para los procesos de administración de riesgos, a fin de apoyar la mejora continua de los datos y procesos de riesgos orientados a TI.
- Métricas y presentación de información de riesgos para contar con una perspectiva continua de la exposición al riesgo.
- Administración de problemas para el manejo de estos de manera operativa.
- Aceptación del riesgo para los riesgos residuales por parte de la Gerencia.
- Administración de amenazas y vulnerabilidad.
- Administración de crisis durante desastres y eventos importantes.
- Concientización y capacitación para mejorar las capacidades con el objetivo de la administración de riesgos de TI

13.- Definición de una política de autoevaluación del Directorio

Los Principios de Gobierno Corporativo de la OCDE establecen que <<El marco para el gobierno corporativo deberá garantizar la orientación estratégica de la empresa, el control efectivo de la Dirección Ejecutiva por parte del Directorio y la responsabilidad de este frente a la empresa y los accionistas>> (Organización para la Cooperación y el Desarrollo Económicos [OCDE] 2004:24). Se sugiere que cada miembro autoevalúe su desempeño y además, comparta sus opiniones sobre el funcionamiento general del Directorio. Los resultados de estas evaluaciones contribuyen a mejorar:

- El funcionamiento del Directorio
- La interacción entre los miembros
- Se identifican las fortalezas y las debilidades en las operaciones del Directorio
- Se identifican las oportunidades de mejora para el Directorio y los directores en general

La Corporación Financiera Internacional [IFC] (2010), nos menciona un modelo práctico utilizado por Ferreyros Corp., que consiste en un cuestionario anónimo que cada miembro del Directorio responde. Las preguntas tratan de cubrir los aspectos referentes a desempeño, asistencia y quórum, importancia de cada sesión, actas de reuniones y aportes de los miembros, entre otros. Posterior a ello, se debe analizar el resultado de la encuesta entre todos los directores y definir planes de acción para mejorar el funcionamiento del Directorio.

14.- Definición de independencia y los criterios definidos a ser considerados en el perfil de los directores independientes.

Los Lineamientos para un Código Andino de Gobierno Corporativo indican que: <<Los Estatutos fijarán los criterios que haya que tener en cuenta en la definición de los directores como independientes. Las personas de reconocido prestigio profesional que puedan aportar su experiencia y conocimientos al Directorio y que, no siendo ni ejecutivos ni directores no independientes, reúnan las condiciones que aseguren su imparcialidad y objetividad de criterio, serán aptos para ser designados como directores independientes.>> (Corporación Andina de Fomento [CAF] 2010:54)

Los criterios para determinar cuándo un director es independiente. Entre los criterios a considerar para clasificar a un director como independiente, se deben tener en cuenta los siguientes:

- No tener, o haber tenido recientemente de forma directa o indirecta y de carácter significativo vínculo laboral, contractual o comercial o contractual, directa o indirecta con la Entidad, sus directivos o los directores no independientes.
- No ser director de otra entidad que tenga directores no independientes en esta Entidad.
- No tener parentesco con los directores ejecutivos, directores no independientes o la Alta Dirección de la Entidad.
- Contar con un perfil personal y profesional que brinde confianza a los promotores en relación con su independencia.

Es recomendable evaluar dentro del Reglamento del Directorio el número mínimo de directores independientes que deberán formar parte del Directorio.

15.- Actualizar y formalizar la Arquitectura de TI

El Marco Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés) nos define lo siguiente: <<La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. >> (IT *Governance Institute* 2007: 33).

Por tal motivo es necesario, actualizar y formalizar la Arquitectura de TI, la misma que consolide los recursos de TI que permiten la integración de las aplicaciones, sistemas, red, bases de datos y recursos de tecnología. Con el objetivo de mejorar la toma de decisiones gerenciales proporcionando información confiable y segura, y administrar adecuadamente los recursos de TI orientándolos a la estrategia del negocio. Al formalizar la Arquitectura de TI se incrementa la responsabilidad sobre la integridad y seguridad de los datos.

Asimismo, COBIT nos menciona que para obtener una adecuada Arquitectura de TI se debe realizar lo siguiente:

- El aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos
- La asignación de propiedad de datos
- La clasificación de la información usando un esquema de clasificación acordado que se mide con : (a) El porcentaje de elementos de datos redundantes/duplicados, (b) El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la empresa y (c) La frecuencia de actividades de validación de datos.

16.- Segregación de funciones a nivel de procesos y sistemas informáticos

Con el fin de disminuir las deficiencias detectadas en cuanto a la segregación de funciones[10] , es necesario conocer qué roles presentan conflictos, identificando como críticos aquellos casos que permiten completar un ciclo completo de operaciones en alguno de los módulos de los sistemas actuales. Se recomienda considerar principalmente las actividades relacionadas con el registro de transacciones, autorización y custodia de activos, así como a aquellos usuarios que tienen acceso al ambiente productivo como al ambiente de desarrollo, ya que en este último caso existe el riesgo de la modificación de datos maestros. Según KPMG Perú (2015) se indican los siguientes pasos a realizar para analizar con mayor profundidad el nivel actual del componente de segregación de funciones:

- Comprender las responsabilidades que son inadecuadas para ciertas descripciones de trabajos.

[10] Control que busca evitar que un colaborador tenga los permisos suficientes para ejecutar dos o más transacciones sensibles o en conflicto que podrían afectar los estados financieros o incrementar el riesgo de fraude.

- Definir responsabilidades apropiadas dentro de las políticas y procedimientos de la Organización para ayudar a promover y apoyar la segregación adecuada de funciones.
- Evaluar los recursos del personal para determinar los mejores enfoques.
- Evaluar y apalancar la tecnología para apoyar una adecuada segregación de funciones.

EY México (2011) indica que ningún colaborador de la Entidad debe tener tantos accesos a los sistemas informáticos que permitan ejecutar transacciones en todo un proceso de negocios sin controles y autorizaciones, debido a que representa un alto riesgo para el negocio.

Por tal motivo es necesario utilizar un enfoque basado en riesgos, el cual permite que las empresas administren el riesgo de fraude y fallas de control interno de una manera equilibrada y eficiente que refleje el valor que están protegiendo. Esta metodología consta de cinco fases:

- Definición a nivel de negocio: identificación de transacciones más sensibles a riesgo de fraudes en la Entidad cuando un colaborador cuenta con acceso excesivo a los sistemas informáticos. Así mismo, se necesita determinar el umbral (riesgo e impacto) por cada posible conflicto de segregación de funciones. El resultado de esta etapa es la Matriz de Conflictos.
- Definición técnica: la Entidad identifica cada transacción sensible definida y las plataformas informáticas que dan soporte a la ejecución de dicha actividad.
- Prueba: se realiza un análisis de usuarios con conflicto de segregación utilizando la información de las 2 anteriores fases y se determina la gravedad de los conflictos en los usuarios por cada área y plataforma informática. Este resultado debe ser informado a la Alta Gerencia y a la Auditoría Interna.
- Mitigación: se procede a limitar la posibilidad de la materialización de riesgos y, en caso fuere necesario, diseñar controles adicionales que mitiguen más aún el riesgo.
- Remediación: en este último paso se rediseñan y depuran los roles, se revisan la idoneidad de los usuarios y se implementa la herramienta de segregación de funciones. Las opción más sencilla es la depuración de roles y el desarrollo de roles implica grandes cambios organizacionales en los colaboradores, procesos y tecnología.

Los principales beneficios que obtendría la Entidad luego de implementar una adecuada segregación de funciones a nivel de proceso y de sistemas informáticos mejorando así los ambientes que sustenta la información operacional y financiera, sería los siguientes:

- Mejorar el ambiente de control interno.
- Mitiga favorablemente las acciones fraudulentas o mal intencionadas en la Entidad.
- Se identifica y otorga acceso a la información sensible de la Entidad a los usuarios adecuados.

- Optimización de los niveles de seguridad en los sistemas de la Entidad al controlar los accesos de usuarios y estableciendo procedimientos para su mantenimiento.

17.- Elaboración de un Plan de Crisis

La Entidad debe elaborar el Plan de Crisis estableciendo las actividades para proveer respuesta a eventos de interrupción operativa que pueda llevar a una crisis. Con la finalidad de gestionar adecuadamente este plan debe contener los siguientes actores:

- Comité de Crisis: encargado de evaluar y gestionar la situación de crisis durante los incidentes sucedidos así como realizar el diagnóstico de la situación, definir y ejecutar el plan de acción con los coordinadores generales. Este comité debe ser presidido por el Gerente General.
- Coordinadores Generales: su principal responsabilidad es comunicar la situación de crisis surgida a los miembros del Comité, realizar seguimiento de los incidentes, activar los planes de continuidad operativa y facilitar a los colaboradores procedimientos básicos para ejecutar sus actividades durante la contingencia.
- Equipo de Soporte: realizar el diagnóstico a nivel de imagen de la Entidad, recopilar información y documentación sobre la contingencia para definir la estrategia de comunicación interna y externa. Además, debe mantener informado al Comité de Crisis el desarrollo de las actividades de comunicación externa.
- Unidades Receptoras: informar al coordinador designado la ocurrencia de una situación de crisis para su resolución y cumplimiento.

Por otro lado, este plan debe contener los siguientes puntos:

- Herramientas de comunicación: cuáles serán los medios formales para informar la situación de crisis.
- Criterio de activación, en el que se define el tipo de alerta que debe ser utilizado al conocer la contingencia.
- Definición del impacto de la operación del negocio causado por no disponibilidad de uno de los subprocesos para proporcionar el servicios. El impacto puede ser de tipo operacional, legal, financiero, imagen institucional, entre otros que considere la Alta Gerencia.

18.- Elaborar un plan de capacitación para el área de Auditoría Interna para la obtención de certificaciones internacionales

El Instituto de Auditores Internos (2013) en la Norma Internacional para el Ejercicio Profesional de la Auditoría Interna 1230 - Desarrollo Profesional Continuado indica que los auditores internos deben perfeccionar sus conocimientos, aptitudes y otras competencias mediante la capacitación profesional

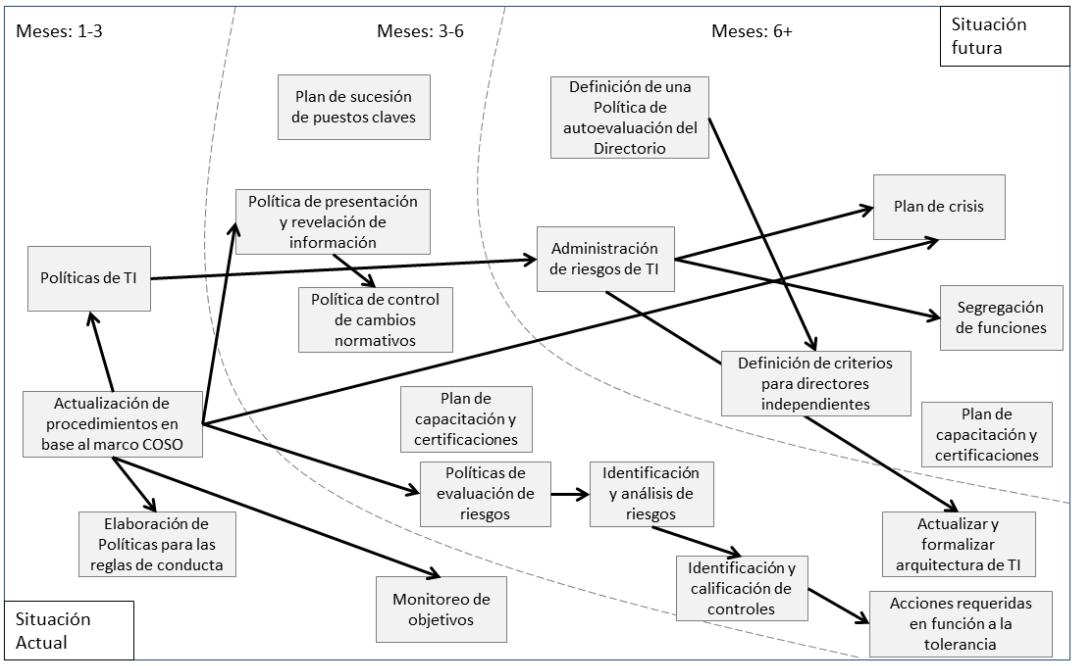
continua y considerando lo mencionado en el Consejo para la Práctica 1230-1 respecto que el Instituto alienta a los auditores internos a demostrar su aptitud mediante la obtención de una certificación profesional apropiada, tal como la designación CIA (Certified Internal Auditor), otras designaciones ofrecidas por el Instituto y otras designaciones relacionadas con auditoría interna. Por tal motivo, es necesario que la Gerencia de Auditoría Interna elabore un plan de capacitación para su personal con el objetivo de obtener una certificación internacional a mediano plazo con la finalidad de incrementar los conocimientos, habilidades y destrezas en el personal del área, generando un mayor valor agregado para la Entidad en los temas relacionados con la administración de riesgos, control y gobernanza.

Capítulo VI. Revisión y priorización de oportunidades de mejora

De acuerdo con las deficiencias de control identificadas en base a los parámetros pauteados por el Marco COSO 2013, y de acuerdo con las entrevistas al el personal de la Entidad, se definieron aquellos puntos más críticos, para los cuales se elaboraron y propusieron los planes de remediación planteados en el Capítulo V.

Se entiende que los recursos de una organización son limitados, y deben estar orientados a la consecución de los objetivos estratégicos de forma eficaz y eficiente, por lo cual se considera óptimo esquematizar el desarrollo de los planes de acción a través de una hoja de ruta que permita a la Entidad contar con una guía para la implementación de los planes de acción recomendados.

Gráfico 5. Hoja de Ruta para implementar los planes de acción



Fuente: Elaboración propia, 2015

Para obtener como resultado la hoja de ruta que se presenta en el gráfico 5, se consideraron otros criterios a fin de evaluar complejidad del desarrollo del plan y el impacto que podría tener la implementación del mismo para levantar una brecha respecto a la situación esperada del sistema de control. La complejidad y el impacto fueron designados en función de una calificación de 3 niveles (alto, medio, bajo), los cuales fueron definidos en función de criterio experto de quienes desarrollamos el presente trabajo y en consideración de los resultados del diagnóstico y de los lineamientos exigidos por el marco seleccionado para la evaluación del Sistema de Control Interno. A continuación se presentan los resultados de la calificación:

Tabla 4. Calificación de planes de acción según complejidad e impacto en el Sistema de Control Interno

N°	Planes de Acción	Complejidad	Puntaje	Impacto SCI	Puntaje
1	Actualización de procedimientos considerando lo indicado en el COSO 2013	Alto	3	AR	3
2	Actualizar y formalizar políticas y procedimiento de TI	Moderado	2	AR	3
3	Elaboración de políticas y reglamentos requeridos por la Entidad para fijar las reglas de conducta	Bajo	1	AR	3
4	Elaboración de una política de presentación y revelación de la información	Moderado	2	AR	3
5	Elaboración de políticas y procedimientos de control de cambios normativo	Bajo	1	MR	2
6	Definir y formalizar medidas de control para el monitoreo de los objetivos	Moderado	2	AR	3
7	Consolidar las políticas de evaluación de riesgos para todos los niveles de la organización	Moderado	2	AR	3
8	Realizar la identificación y análisis de riesgos	Alto	3	AR	3
9	Realizar la identificación y calificación de controles	Alto	3	AR	3
10	Definir y delimitar las acciones requeridas para los niveles de apetito y tolerancia	Moderado	2	R	1
11	Elaboración del “Plan de sucesión de puestos claves”	Alto	3	R	1
12	Administración de Riesgos de TI	Moderado	2	AR	3
13	Definición de una política de autoevaluación del Directorio	Bajo	1	R	1
14	Definición de independencia y los criterios definidos a ser considerados en el perfil de los directores independientes	Moderado	2	R	1
15	Actualizar y formalizar la Arquitectura de TI	Alto	3	R	1
16	Segregación de funciones a nivel procesos y sistemas informáticos	Alto	3	AR	3
17	Elaboración de un "Plan de Crisis"	Moderado	2	MR	2
18	Elaborar un plan de capacitación para el área de Auditoría Interna para la obtención de certificaciones internacionales	Bajo	1	R	1

Leyenda
Altamente Relacionado (AR): El Plan se encuentra estrechamente relacionado con el levantamiento de las observaciones para un Sistema de Control Interno efectivo.
Medianamente Relacionado (MR): El Plan se encuentra vinculado al levantamiento de las observaciones para un Sistema de Control Interno efectivo, sin embargo, puede contemplar otros aspectos relacionados con la gestión integral de riesgos u otros parámetros o metodologías de control.
Relacionado (R): Relacionado con otros parámetros o metodologías de control.

Fuente: Elaboración propia, 2015

Conociendo el grado de complejidad e impacto de cada plan de acción, se procedió a calcular las horas hombres que se utilizarán para llevar a cabo la implementación respectiva, considerando como recursos posibles a personal de los siguientes cargos: Gerente, Supervisor y Asistente. Además, con la finalidad de cuantificar el costo de implementación aproximado se utilizaron como referencia los sueldos promedio de los funcionarios de la Entidad. Con respecto a esta última consideración es preciso detallar que al ser esta información de carácter confidencial se convirtieron dichos importes monetarios a porcentajes, para lo cual se otorgó el “100%” al valor del sueldo de un gerente, por ser este el mayor

valor, y tomando este 100% como base de determinaron los porcentajes que representan el sueldo de un Supervisor y de un Asistente, los que se representaron por 48% y 27.4% respectivamente.

Cabe señalar que el resultado de esta multiplicación, al que se le asignó la denominación de "Factor Horas x (%)" si bien otorga indicios suficientes de los recursos estimados que serán requeridos para el desarrollo de los planes de acción, no condiciona en orden de importancia la hoja de ruta de los planes, ya que esta fue realizada no solo en función de criticidad de planes, sino tomando en consideración la dependencia que existe entre el desarrollo de las actividades. Es decir, se han considerado como iniciales aquellas actividades que están más relacionadas con el levantamiento de observaciones de la situación esperada de control interno, pero teniendo en cuenta que son actividades que son necesarias realizar para poder definir la implementación de otras actividades siguientes. Razón por la cual se puede observar en el gráfico 5 que existen actividades con un mismo o similar valor de "Factor Horas x (%)" que pueden realizarse tanto en el corto como en el largo plazo.

Tabla 5. Estimación de horas hombre y costo de hora para la implementación de los planes de acción

N°	Planes de Acción	Horas Hombre / Costo por Hora						Factor Horas x (%)
		Gerente		Supervisor		Asistente		
		Horas	% por Hora	Horas	% por Hora	Horas	% por Hora	
1	Actualización de procedimientos considerando lo indicado en el COSO 2013	60	100%	180	48%	240	27.40%	212.16
2	Actualizar y formalizar políticas y procedimiento de TI	20	100%	50	48%	80	27.40%	65.92
3	Elaboración de políticas y reglamentos requeridos por la Entidad para fijar las reglas de conducta	60	100%	100	48%	120	27.40%	140.88
4	Elaboración de una política de presentación y revelación de la información	20	100%	40	48%	100	27.40%	66.60
5	Elaboración de políticas y procedimientos de control de cambios normativo	20	100%	40	48%	100	27.40%	66.60
6	Definir y formalizar medidas de control para el monitoreo de los objetivos	40	100%	80	48%	30	27.40%	86.62
7	Consolidar las políticas de evaluación de riesgos para todos los niveles de la organización	100	100%	150	48%	60	27.40%	188.44
8	Realizar la identificación y análisis de riesgos	100	100%	200	48%	480	27.40%	327.52
9	Realizar la identificación y calificación de controles	100	100%	200	48%	600	27.40%	360.40
10	Definir y delimitar las acciones requeridas para los niveles de apetito y tolerancia	40	100%	80	48%	40	27.40%	89.36
11	Elaboración del “Plan de sucesión de puestos claves”	60	100%	60	48%	100	27.40%	116.20
12	Administración de Riesgo de TI	20	100%	200	48%	400	27.40%	225.60
13	Definición de una política de autoevaluación del Directorio	40	100%	40	48%	20	27.40%	64.68
14	Definición de independencia y los criterios definidos a ser considerados en el perfil de los directores independientes	40	100%	40	48%	20	27.40%	64.68
15	Actualizar y formalizar la Arquitectura de TI	20	100%	160	48%	280	27.40%	173.52
16	Segregación de funciones a nivel procesos y sistemas informáticos	100	100%	400	48%	900	27.40%	538.60
17	Elaboración de un Plan de Crisis	15	100%	60	48%	120	27.40%	76.68
18	Elaborar un Plan de Capacitación para el área de Auditoría Interna para la obtención de certificaciones internacionales	10	100%	20	48%	40	27.40%	30.56

Fuente: Elaboración propia, 2015

Conclusiones

El presente documento tuvo como objetivo principal proponer los lineamientos para la adecuación del Sistema de Control Interno sobre la base del Marco COSO 2013 en la Entidad Educativa IFB, con la finalidad de que se prevengan posibles riesgos que puedan afectar la operatividad y continuidad de la Entidad. Asimismo, al contar con un efectivo Sistema de Control Interno, la Entidad incrementa la posibilidad de lograr los objetivos estratégicos establecidos, a la vez que genera mayor eficacia, eficiencia y transparencia en sus operaciones así como logra alinearse a cumplir con el marco normativo en el que se desarrollan sus actividades.

Con la finalidad de definir los lineamientos, se realizó un diagnóstico del nivel de madurez del Sistema de Control Interno utilizando como referencia el nuevo Marco COSO (2013) observando que la Entidad se encuentra en un grado de madurez nivel 2 según la "Tabla de ponderación para la evaluación del nivel de madurez de los componentes de COSO". Asimismo, observamos que los elementos de control interno existen y se encuentran definidos por la Alta Dirección, sin embargo, no se han definido ni parametrizado los ámbitos para su aplicación, disminuyendo la seguridad razonable del cumplimiento de objetivos planteados por la Entidad. Por otro lado, al no contar con ámbitos definidos respecto a la aplicación del control interno, el personal no interioriza ni se encuentra comprometido con esta materia, así como tampoco se responsabiliza por los controles de los procesos de los cuales son responsables, incrementando la posibilidad de sobrecostos, ejecución de actividades innecesarias e ineficiencias en la identificación y remediación de problemas potenciales.

Al conocer el grado de madurez del Sistema de Control Interno de la Entidad, concluimos que los componentes con mayores brechas son "Actividades de Control" e "Información y Comunicación". En el caso de "Actividades de Control" la falencia se da principalmente por una inadecuada segregación de funciones en los sistemas informáticos de la Entidad, los cuales permiten la vulneración de los controles implementados por la Alta Dirección y por cada dueño de proceso. Para el caso de Tecnologías de Información y Arquitectura de la Tecnología, no se cuenta con políticas y procedimientos actualizados y formalizados. Para el otro componente "Información y Comunicación", las brechas son originadas por la falta de identificación de qué información clave es requerida para que los procesos operen y cuál es la información que genera cada una, niveles de responsabilidad en relación con la elaboración y aprobación de la

información que se genera en cada proceso, así como la falta de identificación de información que debe ser de conocimiento público.

La Alta Dirección reconoce que el nivel de madurez del Sistema de Control Interno se encuentra en proceso de implementación a mediano y largo plazo. Sin embargo, al identificar las brechas en el diagnóstico realizado y al conocer el interés de la Alta Dirección en qué aspectos profundizar para mejorar su Sistema de Control Interno, se concluye que para fortalecer la efectividad del funcionamiento del control interno es necesario realizar una priorización de planes de acción ya que los recursos financieros y humanos de la Entidad han sido registrados en el presupuesto del presente año.

De aceptarse los planes de acción y su respectiva priorización, se requiere tener en cuenta la "Hoja de Ruta", la cual organiza el tiempo y establece las actividades a realizar de forma secuencial, considerando las dependencias entre ellas, para alcanzar el objetivo principal, que es fortalecer el Sistema de Control Interno.

Es importante mencionar, que los planes de acción propuestos a la Alta Dirección afectan a más de un componente, de forma directa o indirectamente, generando que los cinco componentes funcionen en conjunto de forma integrada, reduciendo a un nivel aceptable el riesgo de no alcanzar los objetivos de la Entidad.

Finalmente y como un aspecto importante a considerar para la mejora del Sistema de Control Interno, el análisis de viabilidad realizado, en base a las horas hombres estimadas para implementar cada plan de acción, nos indica que el fortalecimiento se irá dando progresivamente a corto, mediano y largo plazo; siempre y cuando la Alta Dirección disponga de recursos suficientes para el desarrollo del proyecto y, a su vez, transmita a la organización, en todos los niveles, la importancia del control interno para alcanzar los objetivos, incrementar los niveles de competitividad por medio de una administración transparente y aumentar la rentabilidad.

Bibliografía

IFB Certus (2015). *Página web de IFB Certus.* http://www.ifbcertus.edu.pe/#nosotros

Organización para la Cooperación y el Desarrollo Económicos (2014). *Principios de Gobierno Corporativo de la OCDE*. Francia.

Corporación Financiera Internacional (2010). *Guía Práctica de Gobierno Corporativo. Experiencias del Círculo de Empresas de la Mesa Redonda Latinoamericana*. Estados Unidos.

Corporación Andina de Fomento (2010). *Los Lineamientos para un Código Andino de Gobierno Corporativo.* Segunda Edición. Colombia.

KPMG Asesores S. Civil de R. L., (2015). *Segregación de Funciones*. [En línea]. Perú. Fecha de Consulta: 04/04/2015. Disponible en: http://www.kpmg.com/PE/es/IssuesAndInsights/ArticlesPublications/Documents/Factsheets/Segregaci%C3%B3n-de-Funciones.pdf

Mancera, S.C. Integrante de Ernst & Young Global (2011). *Un enfoque basado en riesgos para la segregación de funciones*. [En línea]. México. Fecha de Consulta: 07/04/2015. Disponible en: http://www.ey.com/Publication/vwLUAssets/Perspectivas_relacionadas_con_el_riesgo_de_TI/$FILE/Enfoque_basado_en_riesgos_para_la_segregacion_de_funciones.pdf

Mancera, S.C. Integrante de Ernst & Young Global (2012). *Cambios en el panorama de los riesgos de TI.* [En línea]. México. Fecha de Consulta: 07/04/2015. Disponible en: http://www.ey.com/Publication/vwLUAssets/Cambios_en_el_panorama_de_los_riesgos_de_TI/$FILE/Perspectivas_riesgos_TI.pdf

IT Governance Institute (2007). Cobit 4.1. Estados Unidos.

The Institute of Internal Auditors (2006). Guía *para la evaluación de TI* – GAIT. Estados Unidos

The Institute of Internal Auditors (2013). *Marco Internacional para la Práctica Profesional de la Auditoría Interna*. España

Ernst & Young Asesores de S. Civil de R. L. (2014). *Perspectiva sobre Gobierno, Riesgo y Cumplimiento*. [En línea]. Perú. Fecha de Consulta: 07/04/2015. Disponible en: http://www.ey.com/Publication/vwLUAssets/Perspectivas_sobre_Gobierno,_Riesgo_y_Cumplimiento/$FILE/EY-perspectivas-gobierno-riesgo-cumplimiento.pdf

COSO (2013). Control Interno – Marco Integrado *"Herramientas Ilustrativas para Evaluar la Efectividad de un Sistema de Control Interno".*

COSO (2013). Control Interno – Marco Integrado *"Marco y Apéndices".*

EY Turning risk into results, Ernst & Young study, 201: Ernst & Young. (2013). *"EY Turning risk into results"*. Sección Study. En: <http://www.ey.com/Publication/vwLUAssets/Turning_risk_into_results/$FILE/Turning%20risk%20into%20results_AU1082_1%20Feb%202012.pdf>

Anexos

Anexo 1. Tabla de Ponderación para la evaluación del nivel de madurez de los componentes COSO 2013

Componentes Clave del Control Interno	**Inicial (1)**	**En proceso de implementación (2)**	**Establecido / Implementado (3)**	**Avanzado (4)**	**Optimizado (5)**
Ambiente de control	Los elementos de control interno de este componente son incipientes o no están formalizados y no es posible comprobar su ejecución	Algunos elementos de control interno de este componente existen y están definidos de manera general, pero no se han definido ni parametrado los ámbitos para su aplicación	Los elementos de control interno de este componente están definidos y se aplican a las áreas y procesos críticos	Los elementos de control interno de este componente están definidos de manera detallada y formalmente, y se aplica en la mayoría de áreas y procesos críticos	Los elementos de control interno de este componente están definidos de manera detallada y formalmente, y se aplican en todas las áreas y procesos críticos. Se revisa la metodología de control interno periódicamente y se analiza su nivel de beneficio
Evaluación de riesgos					
Actividades de control					
Información y comunicación					
Supervisión					

Fuente: Herramienta de elaboración propia en función de los parámetros definidos para COSO_ERM

Anexo 2. Herramienta para la evaluación de la situación actual del Sistema de Control Interno sobre la base del Marco COSO 2013

COMPONENTE: ENTORNO DE CONTROL			
Principio 1: La organización demuestra un compromiso con los valores de integridad y ética.			
N°	**Enfoque**	**Comentario**	**P**
1.1	**Establece el *"Tone at the top"***	A partir del año 2014 hasta la fecha la Entidad ha desarrollado una estrategia de difusión de valores a todos los niveles de la organización, alumnado, personal administrativo, docentes, gerencias y Directorio; en la cual, mes a mes, se enfatiza uno de los valores de la Entidad (*). Para el caso de docentes y alumnado, se han incluido en cada syllabus los valores a fin de que estos sean tratados en las sesiones iniciales de cada curso. Siendo la Gerencia General la principal encargada de la dirección y monitoreo de esta estrategia a través de visitas inopinada a cada sede que conforma la Entidad. (*) Los valores que la Entidad ha definido son: - Transparencia: Búsqueda de excelencia en todo lo que hacemos - Calidad: Marcamos la diferencia - Respeto: Sinergia y eficiencia en la gestión - Trabajo en equipo: Con quiénes estamos y dónde estamos - Integridad: Nuestra única opción - Enfoque en sus audiencias: Nos preocupamos por lo que necesitan nuestros estudiantes y lo que requiere el mercado laboral La Entidad no ha documentado formalmente las funciones y responsabilidades del Comité de Directorio, Comité de Gerencia y Comité de Auditoría.	2
1.2	**Estable las normas de conducta**	La Entidad cuenta con el documento 'Código de Conducta', publicado a través de su página Web, el cual está dirigido a todo el personal que labora y estudia en la Entidad, así como a los proveedores de la misma. La finalidad del Código, de acuerdo con lo establecido por la Entidad, es comunicar los principios y compromisos éticos primordiales en el cumplimiento de sus actividades y en la toma de decisiones. Así como el reporte obligatorio por parte de colaboradores y alumnos de aquellas actividades que vayan en contra de los fundamentos éticos que el Código describe. Además, se ha definido como parte de las normas de prevención con relación a conducta, que cada integrante de la Entidad firme, año a año, la renovación de su compromiso con el 'Código de Conducta'.	3
1.3	**Evalúa el cumplimiento de las normas de conducta**	Con relación a la evaluación y monitoreo del desempeño, la Entidad ha definido que este parámetro sea evaluado a través de la percepción de la Gerencia y de una evaluación de 360 grados. Como buena práctica la Gerencia ha establecido que estas encuestas no deben ejecutarse con fechas cercanas (antes y después) a las fechas en las que se reparten incentivos a fin de evitar distorsiones en los resultados. Con respecto al alcance de la evaluación se identificó que si bien se evalúa el cumplimiento con respecto a objetivos a nivel operativo, no se incluyen objetivos de cumplimiento de las normas y procedimientos, por tanto, estos factores no son considerados en la evaluación de manera objetiva. Se identificó también que la Entidad a la fecha no cuenta con un Comité de Crisis.	2
1.4	**Aborda cualquier desviación de forma oportuna**	La Entidad cuenta con el canal de 'Gestión Ética' a través del cual se reportan las situaciones vinculadas a cualquier desviación al Código de Conducta. Cabe señalar que la implementación del canal se realizó a partir del año 2014, siendo implementado a proveedores a partir del mes de abril y será implementado progresivamente a alumnos. En caso que se detecten hechos que desvirtúen las normas establecidas por la Entidad, la Gerencia General y la Gerencia de Auditoría son las responsables de indagar y analizar el caso. En el caso de se encuentre pertinente, se requiere también la presencia del Gerente de Administración y Finanzas. Si el caso está vinculado a un cargo de Gerencia, la situación deberá ser elevada al Comité de Ética, en el que además del Gerente General y el Gerente de Auditoría, participan también el Contralor y uno de los Directores independientes. Sin embargo, en las entrevistas con las gerencias y jefaturas se identificó que el personal tiene una ligera percepción de que la Gerencia no se asegura de que los trabajadores conozcan los documentos normativos que regulan las actividades de la Entidad. En las encuestas a las gerencias y jefaturas, declararon no conocer la existencia de un 'Código de Ética', y de principios y valores establecidos por la Entidad.	2

Principio 2: La Junta Directiva demuestra la independencia de gestión y ejerce la supervisión de la evolución y los resultados de los controles internos.			
N°	**Enfoque**	**Comentario**	**P**
2.1	**Establece las responsabilidades de supervisión**	La Entidad cuenta con los siguientes comités de sesiones de frecuencia definida. - Comité de Directorio - Comité de Gerencia - Comité de Auditoría: cuya función está relacionada con el monitoreo del Sistema de Control Interno, tratamiento y revisión de principales riesgos y desviaciones o deficiencias significativas de control, monitoreo de las acciones de corrección, revisión de resultados financieros y reportes de los parámetros de cumplimiento definidos por la Entidad. - Comité de Calidad y Cultura: cuya función está relacionada con el seguimiento de la percepción e interiorización de valores, así como a la gestión de la mejora de los servicio. - Comité de Jefes de Sedes: cuya función está vinculada al monitoreo del funcionamiento de cada sede, así como de los principales problemas que se presenten en la gestión día a día. - Comité de Gerencias y de Áreas: cuya función está relacionada con el monitoreo del funcionamiento de las Gerencias de la Entidad. - Comité de Recursos Humano y Gestión del Talento: cuya función está vinculada al monitoreo de los temas de gestión de personal, y asignación de oportunidades para el mismo. Y con los siguientes Comités de sesiones de frecuencia no definida: - Comité de Investigación - Comité de Retención Con respecto a las responsabilidades, como se indicó en el punto 1.1 no se han documentado formalmente las funciones de cada Comité; sin embargo, se conocen y reconocen los objetivos de funcionamiento. Para propósitos del Informe, se revisaron las actas/informes de los Comités de Directorio, Gerencia y Auditoría.	2
2.2	**Aplica los conocimientos especializados relevantes**	El Directorio de la Entidad se encuentra conformado por profesionales altamente capacitados, con experiencia en diversos sectores económicos y formación moral necesarios para entender las actividades de la Empresa dentro del sector con la finalidad de evaluar adecuadamente y dirigirla con éxito en el largo plazo a la Entidad. Asimismo, cumplen con la suficiente preparación profesional para representar a la Entidad ante los grupos de interés respectivos. Sin embrago, la Entidad no cuenta con una política de autoevaluación del Directorio en la que se defina la periodicidad a evaluar a los Directores vigentes, así como el grado de cumplimiento de las tareas durante el periodo evaluado y además, los aspectos y tareas a cumplir en el siguiente periodo.	3
2.3	**Opera con independencia**	El Directorio de la Entidad cuenta con 3 directores independientes de un total de 7. Si bien actualmente la Entidad cuenta con más de un tercio de directores independientes, dicha cuota no se encuentra oficializada, por lo cual se encuentra susceptible a variaciones. Por otro lado, la Entidad no cuenta con una definición de independencia ni con criterios definidos a ser considerados en el perfil de los directores independientes. De acuerdo con lo conversado con representantes de la Gerencia, los Directores son seleccionados según las condiciones profesionales requeridas para el puesto y sobre la base a la experiencia profesional de cada Director. Lo cual fue revisado mediante investigación de la plana de Directores. El Directorio está conformado por: - Jesús Zamora León - Arturo Núñez - Jorge Basadre Brazzini - Ángel Becerra - Miguel Aramburú - Enrique Gubbins - Leonardo Bacherer	3

2.4	**Proporciona supervisión para el sistema de control interno**	El Comité de Directorio ha delegado los temas de revisión a detalle con respecto al Sistema de Control Interno al Comité de Auditoría, teniendo este por funciones el monitoreo del Sistema de Control Interno, tratamiento y revisión de principales riesgos y desviaciones o deficiencias significativas de control, monitoreo de las acciones de corrección, revisión de resultados financieros y reportes en relación con los parámetros de cumplimiento definidos por la Entidad. Los resultados del Comité de Auditoría son analizados y revisados con el objetivo de que los temas más relevantes y críticos sean elevados a los comités de Directorio a fin de contar con la opinión del Directorio sobre los hechos y acciones definidas en los comités previos. Los comentarios y planes definidos en Comité de Directorio son relevados por el Contralor, quien comunica las acciones a seguir y las solicitudes del Comité de Directorio a la Gerencia de Auditoría para su correspondiente seguimiento.	3
Principio 3: La Dirección establece, con la supervisión del Directorio, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.			
N°	**Enfoque**	**Comentario**	**P**
3.1	**Tiene en cuenta todas las estructuras de la organización**	La Entidad tiene una estructura matricial y ha definido organigramas para documentar y comunicar las líneas de reporte y responsabilidades en base a los requerimientos de cada Gerencia y en función del cumplimiento de los objetivos estratégicos. En las entrevistas con las gerencias y jefaturas de la Entidad se relevó que se tiene una ligera percepción de que la elaboración, la actualización y la difusión de los planes estratégicas no se realizan de acuerdo con los procedimientos formalmente documentados. Se identificó también que si bien existe documentación formal sobre la organización y funciones por puesto, el problema radica en el empoderamiento y *ownership* de las jefaturas, que no interiorizan la responsabilidad por el accionar del personal a su cargo. En el año 2014, la Entidad ha implementado un nuevo ERP, tanto para el *back* como para el *front office*, por lo cual si bien existen manuales de organización y funciones (MOF), estos no han sido en su totalidad actualizados en función de los cambios que representa el pase a producción del ERP. Además, con respecto a la implementación, no se consideró como parte de las actividades iniciales la construcción de la matriz de segregación de funciones, a fin de incluir una matriz adecuada en la etapa inicial de la implementación del ERP.	2
3.2	**Establece líneas de comunicación de información**	Como se indicó en el punto 3.1. la Entidad cuenta con una estructura matricial. En las entrevistas con las gerencias y jefaturas se identificó que se ha difundido de manera correcta la estructura organizacional vigente; sin embargo, un gran número de los encuestados considera que las actividades reales no se encuentran debidamente documentadas y delimitadas en los manuales de organización y funciones (MOF) correspondientes.	2
3.3	**Define, asigna y limita facultades y responsabilidades**	Con respecto a: - Comité de Directorio: no se encuentran formalmente documentadas las responsabilidades, sin embargo, como se desarrolló en el principio 1 en la documentación revisada se encontró evidencia de la ejecución de sus funciones. - Alta Dirección y Personal: actualmente el Directorio y la Alta Gerencia han definido las responsabilidades y límites de autoridad para todos los niveles jerárquicos, dejándolos plasmados en el Manual de Organización y Funciones (MOF). Sin embargo, al existir un cambio después de la implementación del ERP, en muchos casos se identifica una desactualización con respecto a las funciones y responsabilidades, generando confusión en el personal con respecto al alcance de estas. Además, la segregación de funciones no ha sido contemplada en los parámetros iniciales del sistema. - Proveedores: Si bien es cierto que la implementación del canal de gestión ética ha sido implementado en este mes, se observa que en los contratos celebrados con los mismos, no existen cláusulas en los contratos de servicios o acuerdos firmados por ambas partes en el que se especifiquen las expectativas de cada parte y las responsabilidades frente a los servicios prestados, así como las responsabilidades y condiciones del proveedor frente a los niveles de control interno sobre los procesos o actividades del negocio subcontratadas.	2
Principio 4: La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes en alineación con los objetivos de la organización.			
N°	**Enfoque**	**Comentario**	**P**
4.1	**Establece políticas y prácticas**	La Entidad cuenta con procedimientos referidos a la selección y contratación de personal administrativo y docente, plan anual de capacitación y desarrollo de los empleados, cese y desvinculación en el que se detalla el alcance y responsabilidad de las gerencias involucradas en dichos procedimientos frente a los requerimientos de la Entidad. Con respecto al seguimiento de las competencias del personal, se han definido indicadores y metas para el cumplimiento de los objetivos estratégicos, los cuales son monitoreados por la Gerencia de Auditoría e influyen en los resultados de la evaluación del personal. El seguimiento y revisión de resultados de estos indicadores, para el caso de las gerencias, son revisados por el Gerente General con cada uno de los responsables de las gerencias de primera línea.	3

4.2	**Evalúa las competencias disponibles y aborda la falta de las mismas**	Con respecto a la evaluación de competencias y deficiencias, como se indicó en punto 4.1, la Entidad realiza dicha evaluación a través del monitoreo de indicadores operativos y de cumplimiento. Se reconoce que la Entidad evalúa y revisa periódicamente el desempeño laboral de cada empleado, sin embargo, los encuestados manifiestan que no existen adecuados procedimientos para la gestión de recursos humanos, precisando que no se cuenta con la cantidad de personal adecuado, no se elabora o difunde un plan de capacitación para los empleados y la escala remunerativa no se encuentra acorde con cargo desempeñado. En las entrevistas realizadas con las gerencias y jefaturas se relevó que se considera que se han identificado las competencias necesarias para cada cargo de la Entidad, las cuales han sido plasmadas en un documento formal, sin embargo, este se encuentra desactualizado respecto a los cambios surgidos a raíz de la implementación del ERP. Asimismo, se percibe que el personal que ocupa cada cargo de trabajo cuenta con las competencias establecidas o requeridas por los perfiles de cargo; sin embargo, el 44% las desconoce o reconoce que dichas competencias no se desarrollan del todo.	2
4.3	**Atrae, desarrolla y retiene a profesionales**	Con respecto a la selección, la Entidad cuentas con procedimientos para la selección del nuevo personal, sin embargo, no se han identificado indicadores que permitan revisar el nivel de cumplimiento de dichos procedimientos en cuanto al cumplimiento de objetivos de selección vinculados a la calidad y el nivel técnico de cada evaluado. No existe una política formalmente definida para la retención de personal calificado. Sin embargo, en función de cada caso en particular que solicita la renuncia voluntaria y en función de la evaluación de la Gerencia General en coordinación con la Gerencia responsable y Jefatura directa, se analiza el caso y la posibilidad de retención. Para ello, se plantean los beneficios o cambio de condiciones económicas o de desarrollo profesional al colaborador. En referencia al desarrollo la Entidad cuenta con Planes de Capacitación anuales, tanto para el personal administrativo como para los docentes. Sin embargo, se observó que el nivel de cumplimiento para el año 2014 fue del 80%, debido a factores de reevaluación y priorización interna (cumplimiento de objetivos)	2
4.4	**Planifica y prepara la sucesión**	No se cuenta con una estrategia de gestión del talento, en la que se definan y formalicen los planes de sucesión para las gerencias, subgerencias y jefaturas. No se cuenta tampoco con candidatos identificados para la sucesión y formación en caso de puestos críticos, así como también se carece de un plan de desarrollo individual y un programa de liderazgo.	1
Principio 5: La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.			
N°	**Enfoque**	**Comentario**	**P**
5.1	**Aplica la responsabilidad por la rendición de cuentas a través de estructuras, autoridad y responsabilidad**	La Entidad ha definido una estructura matricial, como se indica en el punto 3.1. En cuanto a la responsabilidad y *ownership* de la Gerencia y la Alta Dirección frente al control interno, se observa que las funciones y responsabilidades de cada puesto se encuentran documentadas en el Manual de Organización y Funciones (MOF), sin embargo, este no ha sido actualizado en función de los cambios coyunturales surgidos principalmente por la implementación de los nuevos sistemas informáticos. Por otra parte, el personal no se siente comprometido ni empoderado frente a las responsabilidades de su equipo, por lo cual no interioriza la responsabilidad por el accionar del personal a su cargo. La responsabilidad directa para la gestión y monitoreo del control interno ha sido delegada a la Gerencia de Auditoría, quien coordina de manera frecuente y cercana con la Gerencia General, quien es finalmente responsable de tomar acción en caso surjan desviaciones de control o temas relevantes de control interno. Asimismo, el Comité de Directorio ha aprobado la tercerización de la ejecución del Plan de Auditoría con respecto a la revisión de procesos críticos.	2
5.2	**Establece parámetros de desempeño, incentivos y recompensas**	Como se indicó en el punto 1.3, la Entidad cuenta con una evaluación de 360 que permite evaluar el desempeño de cada colaborador. Además, se cuenta con un set de indicadores de los objetivos operativos y de cumplimiento por área, los cuales son evaluados a nivel de colaborador y revisados y monitoreados por la Gerencia de Auditoría Interna. Para el caso de gerencias, la Gerencia General es la encargada de la revisión con cada uno de los responsables. Al respecto, se identificó que, si bien se evalúan estos dos componentes, aparte de la percepción de la Gerencia, no se cuenta con lineamientos y criterios que permitan evaluar el cumplimiento y nivel de adherencia a un adecuado Sistema de Control Interno.	3
5.3	**Evalúa los parámetros de desempeño, incentivos y recompensas para mantener su relev.**	Anualmente, el Directorio y la Alta Dirección evalúan los parámetros de desempeño, incentivo y recompensas considerando los factores internos y externos de la Entidad con la finalidad de que estos parámetros se encuentren alineados con los objetivos de la Entidad. No solo se evalúa el aspecto económico, sino que se contemplan las posibilidades de ascenso al personal o la atribución de mayor responsabilidad.	3

5.4	**Tiene en cuenta las presiones excesivas**	La Entidad no ha definido controles con respecto a posibles desviaciones al Código de Conducta y normas de la Entidad en la búsqueda del cumplimiento de los objetivos operativos y estratégicos por parte del personal.	1
5.5	**Evalúa el desempeño y recompensa o aplica medidas disciplinarias a los profesionales oportunos**	Como se indicó en el punto 5.4, la Entidad no evalúa como parte de los objetivos operativos y de cumplimiento y de los indicadores y estrategias para el cumplimiento del logro de objetivos estratégicos el nivel de cumplimiento y adherencia a las normas del Sistema de Control Interno (Código de Conducta), y normativa en general de la Entidad.	1
COMPONENTE: EVALUACIÓN DE RIESGOS			
Principio 6: La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.			
N°	**Enfoque**	**Comentario**	**P**
6.1	**Objetivos Operacionales**		
6.1.1	**Reflejan las decisiones de la Dirección**	La Entidad ha definido como sus objetivos estratégicos los siguientes: - Crecimiento: en función de la cantidad objetiva de estudiantes, sedes y carreras. - Rentabilidad: en función de las metas de crecimiento y del incremento del margen del EBITDAR. - Calidad: para garantizar la calidad del alumnado y mantener las estadísticas de empleabilidad de los egresados. - Posicionamiento: para mantener el liderazgo en el área de Banca y Finanzas y conseguir reconocimiento en las nuevas áreas. Para monitorear el cumplimiento de estos objetivos se han definido iniciativas estratégicas a nivel organizacional e indicadores de performance (KPI) que permiten a la Compañía identificar el nivel de alineamiento y desviación con respecto al logro de cada objetivo en el proceso de crecimiento de la Compañía. Con el propósito de que, a través del cumplimiento conjunto de objetivos por área, se logre la consecución de los objetivos de la Compañía, a partir de los objetivos e iniciativas estratégicas, la Alta Dirección ha definido los objetivos operacionales para cada una de las gerencias de línea. Sin embargo se identificó que: - No se han definido las condiciones para aceptar que los objetivos sean modificados, ya sea con respecto a los valores establecidos o al alcance de los mismos. - Si bien se observó que en las actas de Directorio se mencionan los objetivos estratégicos, no se encontró un anexo en el que se especifiquen a detalle los valores o metas definidas para cada objetivo. - Existe documentación en la que se puede observar que algunos parámetros meta de ciertos objetivos fueron modificados y no se encontró documentación formal de las modificaciones realizadas, situación que podría generar una percepción errónea del cumplimiento, así como desvirtuar el propósito del monitoreo de los objetivos.	3
6.1.2	**Considera las tolerancias al riesgo**	A inicios del año 2014, con el propósito de realizar la identificación y evaluación de riesgos a nivel Entidad, se definió el primer mapa de riesgos, en el cual se establecieron como niveles de riesgo los siguientes: bajo, moderado, alto, muy alto y extremo. Para la construcción del mapa, se identificó la venta total del año anterior y en función de ello se definieron percentiles para el cálculo de los niveles de impacto; la probabilidad fue definida también a través de percentiles en función del número de veces que puede ocurrir el evento en el período de un año. Como consecuencia de la evaluación del impacto y probabilidad se definió el apetito y tolerancia al riesgo, estableciendo que todos aquellos riesgos que fueran superiores al nivel moderado deberían ser gestionados; sin embargo, esto no quedó formalmente documentado como parte de los procedimientos y políticas de gestión de riesgos de la Compañía. En cuanto a los valores meta definidos para los objetivos estratégicos, no se observó que se hayan definido niveles de variación por lo que estos serán aceptados, por tanto no se encontró un análisis que respalde la evaluación de la tolerancia para los objetivos operacionales en función de los riesgos identificados para la Entidad.	2

6.1.3	**Incluyen metas de desempeño financiero y de operaciones**	La Entidad cuenta con dos tipos de metas operacionales para alcanzar los objetivos estratégicos y cumplir las iniciativas estratégicas: - Aquellas que se basan en el cumplimiento de valores cuantitativos al cierre de cada caño, generalmente vinculadas al cumplimiento de objetivos financieros como el presupuesto, el EBITDAR y el crecimiento en relación con la venta, entre otras. - Y aquellas que se basan en el cumplimiento de supuestos cuantitativos, que acompañan el cumplimiento de las metas cuantitativas; como por ejemplo la excelencia en la calidad del servicio, integración y optimización de operaciones, entre otras. Con respecto a ello se identificó que si bien se han definido metas para los objetivos, tal como se indicó en el punto 6.1.1, no se documenta la modificación a estas, así como tampoco se han definido las condiciones bajo las cuales estas serán aceptadas y las instancias en las que deben ser presentadas.	3
6.1.4	**Forman una base sobre la cual se asignan recursos**	La Entidad define el presupuesto de cada año tomando como base el plan estratégico y operacional, los documentos que incluyen los objetivos estratégicos, así como los operacionales y financieros respectivamente. Sin embargo, tal como se indicó en el punto 6.1.2 no se observó que se hayan definido variaciones aceptables en los objetivos, por tanto, no es posible identificar que la Entidad utilice el monitoreo de los resultados de los objetivos como *input* para la ponderación de la criticidad del incumplimiento o cumplimiento parcial de objetivos, y de acuerdo con ello desasignar o asignar recursos adicionales, o definir planes mitigantes.	
6.2	**Objetivos de Información Financiera Externa**		
6.2.1	**Cumple las normas contables aplicables**	La Entidad, a través de un acuerdo contractual formalmente documentado, ha definido en concordancia con la consultora que realiza la auditoría financiera los objetivos de información financiera. Asimismo la consultora, firma mundialmente reconocida en el servicio, ha establecido los principios contables aplicables a la Entidad, los mismos que son presentados en el informe de resultados, los que son presentados al Comité de Directorio y Directorio para el respectivo análisis y comentarios. Con el fin de determinar si el resultado de una transacción o actividad financiera ejecutada por la Entidad es relevante o no, se define el concepto de materialidad parra la evaluación de la misma como parte del análisis presentado en los estados financieros auditados. Es importante señalar que como propósito de esta revisión no se analizó a mayor profundidad este aspecto aparte de lo ya indicado en los párrafos precedentes.	4
6.2.2	**Considera la materialidad**		
6.2.3	**Refleja las actividades de la organización**		
6.3	**Objetivos de Información no Financiera Externa**		
6.3.1	**Cumpla las normas y marcos establecidos externamente**	La Entidad ha identificado las normas del Ministerio de Educación aplicables, definiendo a corto y mediano plazo las acciones que permitirán la adecuación de las actividades de la Entidad a los cambios de la regulación ya establecida. Sin embargo, en la revisión de los resultados de la auditoría, se identificaron ciertas falencias con respecto al cumplimiento y adecuación total de ciertos aspectos considerados en las normativas aplicables, los cuales son de conocimiento de la Gerencia, habiendo tomado acción y definido planes de acción que cubren el riesgo de incumplimiento. Por otro lado, si bien es cierto que la Gerencia de Auditoría Interna identifica los cambios normativos que impactan en las actividades de la Entidad, no se identificó un área o responsable designado formalmente del monitoreo de toda la regulación aplicable, así como de la identificación de las versiones actualizadas y cambios potenciales en la regulación, que permita a la Entidad identificar acciones críticas que deberán ser incorporadas como parte de los objetivos operacionales.	2
6.3.2	**Considera el nivel necesario de precisión**	Con respecto al reporte no financiero: - No se han identificado niveles de precisión y valores de tolerancia o desviación de los objetivos operacionales relacionados con criterios establecidos por terceros, como por ejemplo, el cumplimiento de la normativa aplicable. - Como parte de los objetivos operacionales se identificaron acciones, como el "complementar la oferta académica existente" que requieren la revisión, identificación y monitoreo de la normativa del Ministerio de Educación; sin embargo, no se identificaron las acciones a seguir con el nivel de precisión y exactitud suficiente, en el corto, mediano y largo plazo para la consecución de este objetivo operativo.	1
6.3.3	**Refleja las actividades de la organización**		

		- No se cuenta con políticas y procedimientos que permitan clasificar la información sensible y crítica, tanto a nivel de normativas aplicables tales como la protección de datos, aplicable sobre todo a información de estudiantes; o la información con relación al desempeño de la Entidad en la consecución de sus objetivos estratégicos. - No se cuenta tampoco con políticas y procedimientos definidos para la difusión de información en el ámbito interno, es decir, no se ha definido qué información es requerida por los trabajadores de la Compañía para su conocimiento, interiorización y gestión en su ámbito correspondiente o en su aporte al cumplimiento de los objetivos operativos. - No se encontró una memoria anual de la Compañía en los últimos 3 años. Como se sabe la memoria anual permite reflejar la actividad realizada por la Entidad, así como los logros obtenidos en el período. Si bien es cierto existe información difundida a través de la *Web* oficial con relación a la visión, misión, valores, gobierno corporativo, y transparencia, no se encontró información con relación a los logros de la Compañía.	
6.4	**Objetivo de la Información Interna**		
6.4.1	**Refleja las decisiones de la dirección**	La Entidad ha definido un Comité de Gerencia que sesiona mensualmente. Como alcance de estas sesiones se han delimitado los temas que serán tratados con recurrencia, en adición de los temas que por su relevancia son presentados ante dicho Comité, definiendo así la información y reporte con los que cuenta la Gerencia aparte de la información que recibe como parte de sus actividades diarias. Se identificó también, que la información revisada se encuentra principalmente relacionada con los objetivos de ventas y con el seguimiento de los planes de acción definidos por los dueños de cada proceso vinculados a los riesgos no cubiertos u observaciones encontradas, no se observó seguimiento periódico con respecto al cumplimiento de cada uno de los objetivos operativos.	2
6.4.2	**Considera el nivel necesario de precisión**	Como se indicó en el punto 6.3.2, no se cuenta con políticas y procedimientos sobre la gestión de la información, por lo cual no se ha definido el nivel de precisión y exactitud requerido en la información para cubrir las necesidades de los usuarios y que estos, a su vez, puedan gestionar sus áreas/actividades correspondientes en razón del cumplimiento de los objetivos operativos.	1
6.4.3	**Refleja las actividades de las organización**	No se ha definido formalmente cuál es el inventario de reportes, informes e información en general que debe ser elaborada por cada gerencia responsable, así como las instancias que deben acceder a dicha información, por lo cual, no se observa la difusión en el ámbito interno de las actividades que realiza la Entidad, y si estas son realizadas en un rango aceptable.	1
6.5	**Objetivos de Cumplimiento**		
6.5.1	**Reflejan las leyes y regulaciones externas**	Como se indicó en el punto 6.3.1 la Entidad ha identificado las normas aplicables del Ministerio de Educación. Sin embargo, no se encontró un inventario de todas las leyes y regulaciones aplicables a la Entidad, como, por ejemplo, la Ley de Protección de Datos y las normas relacionadas a seguridad, salud y medio ambiente, entre otras. En esto, se identificaron observaciones vinculadas a seguridad y salud en los resultados de la revisión de auditoría vinculada a la gestión de proyectos y nuevas sedes.	2
6.5.2	**Tiene en cuenta las tolerancias al riesgo**	No se identificó, tampoco, que la Entidad haya definido niveles de variación aceptables con relación al cumplimiento de las normas aplicables, en razón de cuánto costo y riesgo representen estas para la Entidad.	
Principio 7: La Organización identifica los riesgos para la consecución de sus objetivos en todos sus niveles y los analiza como base sobre la cual determinar cómo se deben gestionar.			
N°	**Enfoque**	**Comentario**	**P**
7.1	**Incluye los niveles de organización, filial, división, unidad operativa y función**	El año 2014 se realizó el primer taller de identificación y evaluación de riesgos a nivel entidad en el que participaron gerencias y jefaturas de primera línea. En el taller se revisó y definió el universo de riesgos internos y externos a nivel entidad que podrían afectar el cumplimiento de los objetivos estratégicos. En base al listado de riesgos se calificaron a nivel de riesgos inherentes, en función de los criterios de probabilidad e impacto revisados y acordados entre la consultora que facilitó el taller, y la Gerencia de la Entidad. Los rangos para el impacto fueron definidos en función de percentiles que se valorizaron en base a la venta del año anterior. Para el caso de la probabilidad, se definieron los rangos en función de los percentiles sobre la cantidad de veces que puede ocurrir un evento en el lapso de un año. En el año 2015 se observó la actualización de la calificación inherente de los riesgos a nivel entidad, sin embargo, no se identificó una actualización o modificación sobre el alcance de los riesgos ya identificados; tampoco se observó la eliminación o adición de nuevos riesgos emergentes con respecto a la realidad actual de la Entidad, en caso de aplicar, o el sustento de que no se requieren cambios de los	3

		riesgos ya identificados. Sobre los riesgos operacionales, no se cuenta con un inventario de riesgos por procesos, sin embargo, se revisan y evalúan aquellos riesgos inherentes con calificación moderada, alta y extrema para procesos con priorización alta la misma que se desprende de los resultados de cada Plan Anual de Auditoría. Se identificó, sin embargo, que, si bien se realiza la evaluación de riesgos a nivel entidad y a nivel operativo y se definen planes de acción en caso de aplicar, no existe una metodología que permita correlacionar la materialización de los riesgos operativos con la medida en que esto podría afectar el cumplimiento de los objetivos estratégicos y objetivos operativos para el siguiente año.	
7.2	**Analiza factores internos y externos**	Se revisaron los riesgos a nivel entidad y se observó que estos consideran tanto factores internos como externos que pudiesen afectar los objetivos estratégicos. Con respecto al posible impacto, como se detalló en el punto 7.1.1, la calificación de riesgos se realiza a nivel inherente con respecto a los criterios de probabilidad e impacto, con relación a cuanto podrían afectar a os objetivos estratégicos.	3
7.3	**Involucra a los niveles apropiados de la Dirección**	Como se indicó en el punto 7.1.1, los riesgos a nivel entidad fueron definidos y evaluados por las gerencias y jefaturas de primera línea. Los riesgos a nivel operativo, en cambio, son identificados por la consultora a cargo de la auditoría de ciertos procesos y validados por el gerente de área responsable del proceso a ser evaluado. Las evaluaciones, en ambos casos, son realizadas bajo criterio experto ya que no se cuenta con historia sobre los eventos ocurridos para determinar con mayores luces niveles de probabilidad o impacto sobre los riesgos inherentes. Los riesgos operativos residuales son identificados a partir de los resultados de la evaluación a nivel de diseño y efectividad de las actividades de control relacionadas con cada riesgo en base a una metodología definida que permite calificar el resultado de la evaluación de control y determinar en qué medida afecta el riesgo, para así, obtener la calificación del riesgo residual. Los riesgos a nivel entidad residuales son resultado de la revisión del inventario de riesgos a nivel Entidad realizada en el año 2014, en la que para aquellos riesgos con calificación alta y extrema se solicitaron las acciones definidas para la mitigación de los mismos, en base a ello y a un análisis cualitativo realizado por la consultora, la Gerencia de Auditoría y la Gerencia de Contraloría de la SAFI se identificó el nivel residual de los riesgos revisados.	3
7.4	**Estima la importancia de los riesgos identificados**	Como se indicó en el punto 7.1.1, la criticidad de los riesgos es definida de acuerdo con la combinación de los criterios de impacto y probabilidad, para los cuales se definieron valores porcentuales en base a las estimaciones de ventas y a la probabilidad de ocurrencia respectivamente. Sin embargo, no se cuenta con la historia de la ocurrencia de riesgos materializados que podría permitir una evaluación más objetiva de los niveles de ocurrencia a ser evaluados. La Entidad considera como tolerancia al riesgo que todos aquellos riesgos que fueran superiores al nivel moderado deberían ser gestionados, a pesar de esto, no se encontró una documentación formal en la que se definan las acciones a seguir y cómo o con qué tipo de control se deberán reducir, mitigar o controlar los riesgos, como parte de la gestión de riesgos de la Entidad.	3
7.5	**Determina cómo responder a los riesgos**		

Principio 8: La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.

N°	Enfoque	Comentario	P
8.1	**Tiene en cuenta distintos tipos de fraudes**	Entre los riesgos definidos por la Entidad, se incluyen los riesgos por posibilidad de fraude: - Incumplimiento de políticas y procedimientos para la ejecución de los procedimientos del negocio - Que se presenten activos faltantes por robo, fraude o pérdida - Que se presenten usos inadecuados de los activos e información de la Entidad - Posibilidad de sanciones por incumplimiento de normas regulatorias - Que se presenten operaciones inadecuadas o malintencionadas por falta de control de accesos y permisos de modificación en los sistemas - Que la imagen de la Entidad se vea afectada debido a publicidad engañosa - Incumplimientos regulatorios, procesos legales o malas prácticas Estos riesgos forman parte de los riesgos en la Entidad evaluados y calificados a nivel de probabilidad e impacto inherente, incluidos en los resultados del taller anual de evaluación de riesgos. Además, son revisados en la medida en que se encuentren relacionados con los procesos críticos priorizados como parte del Plan Anual de Auditoría. En cuanto a identificar la materialización de riesgos relacionados con	2

		la posibilidad de fraude, aparte de las revisiones periódicas de auditoría interna, la Entidad cuenta con una política y un canal de línea ética que sirve para comunicar en forma anónima cualquier preocupación sensible o seria relacionada con potenciales irregularidades e incumplimientos del Código de Conducta de la Entidad. El Código de Conducta está a cargo del Comité de Ética de la Entidad, el cual se encuentra compuesto por el Gerente General, Gerente de Administración y Finanzas y Gerente de Calidad y Auditoría. El Comité tiene como parte de sus funciones el atender cualquier consulta o denuncia relacionada con la infracción de los principios planteados en el Código, quienes resolverán de acuerdo con la gravedad del caso o delegando a las instancias correspondientes. Sin embargo, como parte de los resultados de las encuestas a jefaturas y gerencias, se identificó que el 18% del personal tiene la percepción de que la Gerencia no se asegura de que el personal conozca los documentos normativos que regulan las actividades de la Compañía. Con respecto al monitoreo de posibles acciones fraudulentas por terceros, la Entidad no cuenta con procedimientos definidos que permitan establecer controles a fin de monitorear el nivel de cumplimiento de las normas éticas por parte de proveedores, que en caso de incumplimiento podrían afectar negativamente a la Entidad. Con relación a la organización, la Entidad no cuenta con un oficial de cumplimiento. No se identificó, como parte de los reportes presentados al Comité de Auditoría o Directores, el resumen de los hechos que podrían relacionarse con actividades fraudulentas, ya sea por informes elaborados erróneamente o con omisiones de forma premeditada, transacciones no recurrentes, actividades que vayan en contra de los controles definidos y transacciones realizadas que no tengan controles de segregación de funciones, entre otros. Ver punto 8.1.3. Con respecto a la posible elución de controles por parte de la Dirección, la Entidad no ha definido formalmente que toda acción o actividad que represente una excepción o desviación de control, como resultado de una decisión de la Gerencia o de algunas de las gerencias, deba ser presentada a un ente revisor, como el Comité de Auditoría, por ejemplo.	
8.2	**Evalúa los incentivos y las presiones**	Si bien la Entidad ha identificado riesgos relacionados con acciones fraudulentas, en términos generales, se observó que no se han identificado todas aquellas actividades o condiciones que pudiesen incentivar, promover o presionar al personal para que cometan acciones fraudulentas. Con relación a programas de compensación, por la naturaleza de sus operaciones, la Entidad cuenta con procesos en los que los pagos al personal se encuentran condicionados en función de variables, como por ejemplo, el pago a los ejecutivos de ventas por la colocación de matrículas. Con respecto a ello, si bien existen programas de compensación en los que se revisa el desempeño del personal, no se han identificado controles relacionados con la validación del otorgamiento de variables/incentivos en función del monitoreo de posibles acciones fraudulentas para lograr objetivos operativos. En relación también a la compensación, la Entidad no cuenta con un control que permita distinguir los umbrales de cambios significativos en los aumentos de la compensación del personal.	2
8.3	**Evalúa las oportunidades**	Como parte de los documentos que sustentan los principios del buen gobierno corporativo, la Entidad cuenta con el Código de Conducta, que tiene como objetivo definir los principios para comunicar los principios y compromisos éticos para el cumplimiento de las actividades del personal y la toma de decisiones involucradas en ellas. Entre los lineamientos que estable el código se encuentran: - Principios de transparencia e integridad en las acciones vinculadas al uso de recursos, a la aceptación de beneficios o regalos, al robo o al fraude. - Cumplimiento de leyes y regulaciones relacionadas con el reporte de cualquier acto irregular o de cualquier tipo de soborno. - Uso responsable de la tecnología en cuanto a la utilización de recursos solo para fines autorizados. - Relaciones con funcionarios públicos y contribuciones políticas en relación con brindar información exacta a los organismos estatales. - Integridad de informes financieros y reportes operativos en relación con el oportuno y correcto registro de las transacciones y operaciones con el fin de entregar un adecuado reporte financiero que refleje la situación real de la Institución. - Protección de la información reservada y propiedad intelectual en relación con la información que no deberá ser divulgada a terceros para beneficio personal o de terceros. Si bien se cuenta con una metodología de evaluación de riesgos, no se incluye, como parte de la misma, los siguientes aspectos: - La definición de mecanismos que permitan la identificación y monitoreo de cuentas sensibles que podrían estar afectas a una mayor incidencia o probabilidad de eventos de fraude, como, por ejemplo, las cuentas de inventarios, o los pagos variables por los incentivos por venta. - La revisión periódica de aquellas transacciones realizadas bajo el esquema de "excepciones a los procedimientos", ejecutadas en plazos cortos que no permiten la revisión del alcance de las mismas por los entes superiores correspondientes. - Revisión de esquemas automatizados, relacionados con posibles vulnerabilidades del sistema o ventanas para eludir los controles definidos. - Revisión de entradas manuales versus posibilidad de registros automáticos.	2
8.4	**Evalúa las actitudes y justificaciones**		

Principio 9: La organización identifica y evalúa los cambios que podrían afectar significativamente al Sistema de Control Interno.			
N°	**Enfoque**	**Comentario**	**P**
9.1	**Evalúa los cambios en el entorno externo**	Como se indicó en el punto 7.1.1, en el año 2015 se observó la actualización de la calificación inherente de los riesgos a nivel entidad; sin embargo, no se identificó una actualización o modificación sobre el alcance de los riesgos ya identificados; tampoco se observó la eliminación o adición de nuevos riesgos emergentes con respecto a la realidad actual de la Entidad, en caso de aplicar, o sustento de que no se requieren cambios con respecto a los riesgos ya identificados. Asimismo, la Entidad no cuenta con procedimientos o con un sistema de alertas que le permitan identificar información que se relacione con la existencia o aparición de nuevos riesgos. Con respecto a las nuevas tecnologías, el año 2014, la Entidad implementó un nuevo sistema ERP, tanto para el *back* como para el *front office*, sin embargo, no se realizó una identificación formal de riesgos a nivel operativo a fin de cubrir con controles todos aquellos aspectos que hayan podido representar un riesgo	2
9.2	**Evalúa los cambios en el modelo de negocio**		
9.3	**Evalúa cambios en la Alta Dirección**		
COMPONENTE: ACTIVIDADES DE CONTROL			
Principio 10: La Organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.			
N°	**Enfoque**	**Comentario**	**P**
10.1	**Se integra con la evaluación de los riegos**	Anualmente, IFB Certus a partir de la evaluación de los riesgos a nivel entidad y otros criterios de priorización, entiéndase como procesos previamente auditados, juicio de la gerencia y materialidad, identifica los procesos críticos de la Entidad, los cuales son incluidos como parte del Plan de Auditoría Anual. Durante la evaluación de los procesos críticos, se identifican los riesgos moderados, altos, muy altos y extremos por los que se realizan pruebas de efectividad de los controles. El diseño de los controles se encuentra a cargo de un consultor externo, quien realiza esta tarea en concordancia con la gerencia responsable de cada proceso. En cuanto a los riesgos de nivel bajo, la Alta Dirección ha definido asumir el impacto; sin embargo, en la revisión anual del inventario de riesgos se realiza la revaluación del nivel de criticidad de cada riesgo. De acuerdo con los resultados de la efectividad de los controles se identifica el nivel de madurez. En aquellos casos en los que se identifique deficiencia, se solicita planes de acción a los dueños de los procesos evaluados y así se logra fortalecer los controles. El área de Auditoría Interna es la responsable de realizar el seguimiento y verificar la correcta implementación de los planes de acción a fin de mantener los niveles de los riesgos identificados dentro de la tolerancia a nivel entidad definida por la Alta Dirección y en coordinación con cada dueño del proceso. Para evidenciar la correcta implementación de los planes de acción, Auditoría Interna revisa la evidencia (documentos, mejoras en el sistema, entre otros) enviada por cada dueño del proceso. Se identificaron las siguientes debilidades: - Los dueños de los procesos no se encuentran totalmente concientizados para asumir la responsabilidad de la correcta y oportuna ejecución de los controles. - No se ha establecido formalmente en políticas o procedimientos respecto al plazo máximo para entregar la documentación de los planes de acción, así como los requisitos mínimos de esta. - La metodología de Auditoría Basada en Riesgos se encuentra siendo utilizada aproximadamente desde hace año y medio, por tal motivo se encuentran deficiencias en la revisión de la documentación enviada por los dueños del proceso.	3
10.2	**Tiene en cuenta factores específicos de la organización en cuestión**	Como se indicó en el punto 10.1, la Alta Dirección define y desarrolla las actividades de control en función de la naturaleza de sus operaciones mediante la evaluación anual de riesgos a nivel entidad, lo que conduce a la priorización de riesgos críticos y la evaluación de controles relacionados con los procesos que transversalmente son impactados por dichos riesgos. Aparte de esto, en las sesiones del Comité de Auditoría se identifican aquellas actividades de control que requieren revisión o monitoreo con la finalidad de que estos resultados sean reportados en las siguientes sesiones. La Entidad no ha identificado nuevos riesgos después de la implementación de la plataforma informática, lo cual puede generar que las actividades de control no se encuentren orientadas a posibles riesgos calificados como críticos, de acuerdo con el entorno actual de la entidad.	3

10.3	**Determina los procesos de negocio relevante**	Anualmente, la Alta Dirección realiza el "Taller de Riesgos" en el que se presentan los riesgos a nivel entidad y, a su vez, son evaluados con una escala del 1 al 5 (Bajo, moderado, alto, muy alto y extremo) por las gerencias de primera línea, considerando la probabilidad y el impacto de cada uno de ellos. Luego, los resultados son ponderados identificando los riesgos más críticos y después, se complementa con otros criterios de priorización (juicio de la Gerencia (*), materialidad y procesos previamente auditados, entre otros). Finalmente, los riesgos son vinculados y tabulados por cada proceso y como producto de ello, se obtiene un listado de procesos críticos que deben ser priorizados en la evaluación del control interno. El resultado de esta evaluación es presentado al Comité de Auditoría para la aprobación respectiva. La Entidad no cuenta con una cadena de valor formalmente definida, sin embargo, procede a realizar la evaluación de riesgos a través de un inventario de procesos por áreas y no por procesos transversales. (*) El Juicio de la Gerencia considera las opiniones de la Gerencia General con el fin de identificar alguna nueva priorización (Expectativas de un proceso, nueva normativa, implementación de nuevos sistemas y solicitudes del Directorio, entre otros).	3
10.4	**Evalúa distintos tipos de actividades de control**	A la fecha, la Entidad ha automatizado ciertos controles pero existen controles manuales para las validaciones de actividades críticas, como por ejemplo, validación de la planilla de docentes y administrativos, revisión de los Estados Financieros y revisión y seguimiento del presupuesto anual, entre otros. El proceso de automatización de controles se inició con la implementación de nuevas plataformas informáticas, como por ejemplo, *People Soft (Back Office) y Campus Solution (Core* del negocio); sin embargo, estos tienen fallas al no contemplar la segregación de funciones en cada plataforma. Para el caso de los riesgos a nivel entidad que no se encuentran relacionados directamente con los procesos del negocio y no se incluyen dentro del Plan Anual de Auditoría Interna, se definen los planes de acción y anualmente se revisa el grado de avance de estos; en caso de no existir planes de acción relacionados, se procede a la elaboración e implementación de uno. Si bien se ha realizado el inventario de riesgos y se ha vinculado con los objetivos estratégicos no se han definido riesgos orientados a objetivos de procesamiento de información, como por ejemplo: a) integridad con relación a la deficiencia de procesamiento de transacciones internas y con terceros, b) exactitud con relación al adecuado y oportuno registro en el procesamiento de información, c) validez con relación a corroborar la ejecución de eventos de acuerdo con los procedimiento definidos por la Entidad y d) tiempo de respuesta para la toma oportuna de decisiones.	2
10.5	**Tiene en cuenta a qué nivel se aplican las actividades**	En cada proceso del negocio, la Alta Dirección y las gerencias de primera línea son las responsables de mitigar los riesgos relacionados con los procesos, a través del diseño y ejecución de controles que salvaguarden los activos de la empresa y evitan pérdidas económicas o daño a la imagen de la Entidad. Estos controles pueden estar documentados en las políticas y procedimientos establecidos en cada proceso. Adicionalmente, las gerencias son las encargadas de supervisar la correcta y oportuna ejecución de los controles establecidos. El Comité de Auditoría junto con la Gerencia de Auditoría Interna realiza el seguimiento e identificación de los planes de acción por los riesgos a nivel Entidad. Sin embargo, durante la evaluación encontramos que no todos los procesos claves cuentan con políticas definidas; asimismo los procedimientos existentes no se encuentran actualizados debido a la implementación de los nuevos sistemas informáticos, lo cual genera un desconocimiento parcial de las nuevas actividades y las responsabilidades a ser desarrolladas por parte del personal.	3
10.6	**Aborda la segregación de funciones**	La Entidad no ha documentado el análisis de segregación de funciones para cada uno de los procesos críticos o expuestos a riesgos. Tampoco ha analizado y documentado cada una de las actividades expuestas a error o fraude, a fin de asignarlas a distintos equipos de trabajo o personas. Los nuevos sistemas *People Soft y Campus Solution* no fueron parametrados de acuerdo con la segregación de funciones necesaria. Sin embargo, la Entidad, a través de Auditoría Interna, está gestionando un proyecto para implementar una matriz de roles y responsabilidades que permitirá relacionar actividades realizadas por los miembros del departamento de TI y personal administrativo y docente para detectar posibles conflictos de segregación de funciones. Según las entrevistas realizadas, las jefaturas tienen la percepción de que no se han definido, actualizado ni difundido los procedimientos de aprobación y autorización de las actividades y tareas realizadas en los procesos de la Entidad. Por otro lado, no se efectúa la rotación periódica del personal asignado en puestos susceptibles a riesgos de fraude. Tampoco se han definido alternativas de control o controles de compensación para aquellas actividades críticas.	1

Principio 11: La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.			
N°	**Enfoque**	**Comentario**	**P**
11.1	**Establece la dependencia existente entre el uso de tecnología en los procesos de negocios y los controles generales sobre la tecnología**	A la fecha, el departamento de TI no cuenta con una metodología para el aseguramiento de la calidad formalmente documentada con respecto a los servicios prestados a las áreas usuarias de la Entidad. Se incrementa la posibilidad de que no se cumplan las fases y etapas definidas para propiciar tanto la detección de problemas oportunamente, el cumplimiento de los estándares de calidad, como, también, los procedimientos y planes definidos por el mismo departamento. La Entidad no cuenta con una matriz de roles y responsabilidades (matriz "RACI") que permita relacionar entre sí las actividades realizadas por los miembros del departamento de TI para detectar posibles conflictos de segregación de funciones, pudiendo generar lo siguiente: - Posible incumplimiento de procedimientos internos a causa de una inadecuada segregación de funciones en el departamento de TI acorde con los objetivos de la Entidad. - Existencia de funciones no segregadas en el departamento de TI, así como que existan roles y privilegios excesivos en las funciones de los usuarios administradores. La Entidad no ha definido los controles de aplicación como parte de la evaluación de la confiabilidad de las tecnologías vigentes; es decir, los controles que permitan identificar el adecuado funcionamiento de los sistemas implementados y mitiguen los riesgos implicados en el procesamiento de transacciones, por ejemplo, no cuentan con los activos, la base de datos de los cambios en programas y no se realiza un análisis de las principales incidencias en las contraseñas, entre otros.	1
11.2	**Establece actividades de control relevantes sobre las infraestructuras tecnológicas**	La Entidad no cuenta con documentación detallada de la arquitectura de TI para asegurar la solidez, integridad, escalabilidad y flexibilidad de las nuevas tecnologías de solución e integración con las soluciones existentes (p.e. pistas de auditoría, tipo de aplicaciones, servicios, medios de respaldo de información e interfaces) por lo cual no se puede contar con posibilidad ante un incidente que afecte la integridad de la información y tener la trazabilidad histórica de lo sucedido. Adicionalmente, el no contar con una documentación actualizada conduce a que frente a un cambio en el entorno tecnológico o procedimental, existan riesgos de TI que no se estén cubriendo de manera apropiada, lo cual podría comprometer la integridad, confidencialidad y disponibilidad de la información de la Entidad. Al no evaluar y administrar los riesgos de TI adecuadamente, origina que no se cuente con una solución de alta disponibilidad en los enlaces primaros de conexión a Internet que garantice la conexión con los servicios de TI alojados en la nube. Esta situación generaría la imposibilidad de acceso a los sistemas de información alojados en la nube, afectando las operaciones del negocio, así como pérdidas económicas por no contar con acceso a los sistemas de información críticos. Tampoco se cuentan con procedimientos de planes de recuperación de información así como planes de recuperación frente a desastres.	1
11.3	**Establece actividades de control relevantes sobre los procesos de gestión de la seguridad**	Como se detalló en el enfoque anterior 11.2, no se encuentra detallada la arquitectura de TI para asegurar la solidez, integridad, escalabilidad y flexibilidad de las nuevas tecnologías de solución, e integración con las soluciones existentes. En las evaluaciones del periodo 2014, Auditoría Interna observó la existencia de cuentas de personal de TI con acceso a funciones de negocio en el sistema *People Soft* con lo cual se genera un conflicto en las segregación de funciones. Adicionalmente, se identificaron la existencia de cuentas de personal encargado del proyecto de la implementación del nuevo sistema de información *People Soft* que tienen acceso administrativo total sobre la información. Al no existir actividades de seguridad que se encuentren orientadas a limitar el acceso de los sistemas, redes y aplicaciones en general a aquellos colaboradores que no lo requieran por la necesidad del negocio, generando una posible falencia en la confiabilidad de la información. Tampoco se han identificado riesgos y controles a las amenaza externas vinculadas al uso de la tecnología lo que conduce a una exposición de la información sensible de la Entidad (datos del alumnado, presupuestos por áreas y planillas, entre otros). No se ha realizado una revisión de los permisos de acceso y contrastándolos contra las políticas de otorgamiento de usuarios y perfiles con la finalidad de validar que estos sean correctos.	1
11.4	**Establece actividades de control relevantes sobre los procesos de adquisición, desarrollo**	Como se indicó en enfoque 11.1, el área de TI no cuenta con una metodología para el aseguramiento de la calidad formalmente documentada con respecto a la adquisición, desarrollo y mantenimiento de servicios soportados por tecnologías o sistemas informáticos, así como tampoco se cuenta con una política de niveles de acuerdos de servicios que permitan proteger a la Entidad frente al incumplimientos de plazos, alcance y calidad brindados por terceros o personal interno referidos a la implementación o actualización de los sistemas. Tampoco se han definido políticas y procedimientos para escoger proveedores para la selección o modificación de sistemas.	1

Principio 12: La organización despliega las actividades de control a través de políticas que establecen las líneas generales de control interno y procedimientos que llevan dichas políticas a la práctica.			
N°	**Enfoque**	**Comentario**	**P**
12.1	**Establece políticas y procedimientos para respaldar la implantación de las instrucciones adoptadas por la Dirección**	Si bien la Entidad cuenta con documentos normativos internos (políticas y procedimientos, entre otros) que norman y establecen lineamientos para la ejecución de los procedimientos, existen algunos procesos para los cuales no se han emitido lineamientos que reflejen la visión de la Alta Dirección con respecto a las actividades de control que se deberán llevar a cabo para el logro de los objetivos respetando los niveles de tolerancia definidos por la Entidad. Adicionalmente, con la implementación de los nuevos sistemas informáticos *People Soft (Back Office) y Campus Solution* (Procesos *Core* del negocio) la documentación elaborada se encuentra desactualizada al no contemplar las nuevas funciones que tiene el personal administrativo y docente. Los lineamientos emitidos para normar los procedimientos, así como la documentación de procesos con que cuenta la Entidad no ha sido elaborada bajo el enfoque de control interno, los procesos, actividades y tareas no cuenta con documentación que describa: - Dueño del proceso - Riesgos inherentes al proceso y controles existentes que ayuden a mitigarlos. - Plantillas/matrices de evaluación de la segregación de funciones en cada proceso crítico.	2
12.2	**Establece responsabilidades sobre la ejecución de las políticas y procedimientos**	La Alta Dirección ha designado como responsables directas a las gerencias de línea para administrar los riesgos que afectan a sus procesos respectivamente. Las gerencias tienen la función de designar los responsables de la ejecución de los controles y realizar el monitoreo respectivo dentro de sus áreas; sin embargo, las gerencias son responsables de presentar los avances al Directorio respecto al Sistema de Control Interno así como de implementar los planes de acción correspondientes.	2
12.3	**Se efectúa en el momento oportuno**	Las funciones de evaluación y monitoreo de control interno han sido delegadas a la Gerencia de Auditoría Interna, la cual evalúa periódicamente y según criterio de la Gerencia, los controles implementados en la Entidad; sin embargo, no se ha elaborado el universo de controles a nivel proceso y por tal motivo, no se tiene definida formalmente la periodicidad en que se debe recorrer el 100% de los controles, lo cual incrementa el riesgo de que las evaluaciones no se realicen oportunamente y esto puede involucrar la desnaturalización de aquellos controles preventivos, convirtiéndolos en solo detectivos. Respecto a las medidas correctivas, se identificó una deficiencia en el manejo de tiempos para la ejecución de medidas correctivas debido a que no se han formalizado los plazos máximos para levantar una observación formulada por Auditoría Interna, Auditoría Externa o cualquier ente fiscalizador. No se encuentran definidos formalmente mecanismos de comunicación entre las áreas operativas y el área de Auditoría Interna para informar sobre las mejoras del diseño de control o cambios en los procesos del negocio a excepción de los planes de acción informados posteriormente a las auditorías realizadas.	2
12.4	**Adopta medidas correctivas**	El Directorio ha designado al área de Auditoría Interna como responsable de realizar el seguimiento de las mejoras de las deficiencias de control encontradas durante las auditorías a través de los planes de acción. El cumplimiento de los planes es presentado al Comité de Auditoría detallando principalmente los planes vencidos y se mencionan los planes remediados. Sin embargo, no se ha definido formalmente cuántas veces se pueden modificar la fecha de implementación de un plan de acción y quién será el funcionario responsable de aprobar dicho cambio; tampoco se ha establecido si los dueños de los procesos involucrados deban definir controles mitigantes en caso de replantear dicho plan. Adicionalmente, no se ha formalizado la documentación mínima a entregar por parte de las áreas operativas utilizando formatos modelo y dependiendo de la materialidad.	3
12.5	**Se pone en práctica a través de personal competente**	La Entidad cuenta con un área de Auditoría Interna, la cual se encuentra conformada por un Gerente de Auditoría Interna quien depende directamente del Comité de Auditoría, un Jefe de Auditoría Interna, un Auditor Senior y un Asistente de Auditoría. La Gerencia cuenta con experiencia mayor a los 5 años en el sector y realiza evaluaciones continuas de la calidad y adecuación de los sistemas informáticos y los mecanismos establecidos por la Entidad para garantizar la seguridad de la información; evalúa la implementación oportuna y adecuada de las recomendaciones y medidas para superar las observaciones y recomendaciones formuladas por los auditores externos y realizadas por la propia Gerencia de Auditoría Interna. Dentro de los integrantes observamos que ninguno cuenta con alguna certificación internacional que respalde el conocimiento, las habilidades y las destrezas del auditor interno para a la práctica de la actividad de auditoría interna.	3

12.6	**Revisa las políticas y procedimientos**	Trimestralmente se realiza el Comité de Auditoria, conformado principalmente por directores independientes; como parte de la agenda, se presenta el resultado de las auditorías realizadas en el periodo de evaluación en el que se revisan los riesgos de mayor nivel así como las deficiencias de control encontradas y los compromisos de cada gerencia frente a los riesgos identificados o materializados. El Comité discute el nivel de madurez con referencia al Ambiente de Control de cada proceso evaluado, otorgando una calificación con una escala del 1 al 5 (Bajo, medio, alto, muy alto y extremo). En en caso de que lo consideren necesario, los Directores pueden solicitar o indicar planes de acción, referidos a los riesgos materializados, a las Gerencias respectivas.	2
COMPONENTE: INFORMACIÓN Y COMUNICACIÓN			
Principio 13: La Organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.			
N°	**Enfoque**	**Comentario**	**P**
13.1	**Identifica requisitos de información**	La Entidad cuenta con información que es analizada y evaluada para la toma de decisiones como son: 1. Plan Estratégico, 2. Plan Táctico, 3. Presupuestos y 4. Estados Financieros. Cada área operativa tiene conocimiento parcial del tipo de información que dispone dentro de sus procesos y que sirve para la gestión de sus funciones; esto surgen a raíz de la implementación de los nuevos sistemas informáticos (*PeopleSoft y Campus Solution*). Además, no existen normas internas que regulen las siguientes funciones y característica de la información: integridad, oportunidad, actualización, exactitud, accesibilidad, certidumbre, racionalidad y objetividad. La Entidad no ha identificado cuál es la información clave requerida para que el proceso opere y cuál es la información que genera el proceso. Asimismo, no ha identificado cuáles son los niveles de responsabilidad en relación con la elaboración y aprobación de la información que se genera dentro de cada proceso. Por otro lado, no se ha evaluado la confiabilidad de los sistemas a fin de conocer la pertinencia de la información que se obtiene a partir de ellos para propósitos de análisis, presentación de resultado y comunicación a la Alta Dirección. Se identificaron las siguientes debilidades: - No se han definido mecanismos que permitan identificar las necesidades de información en las diferentes unidades de negocio. - No se evidencia un análisis en el que se concluya que todas las funciones que se realizan dentro de la Entidad cuentan con la información necesaria. - No se cuenta con políticas sobre la información y responsabilidad.	1
13.2	**Capta fuentes de datos internos y externos**	La Entidad utiliza información externa para realizar un mejor análisis del desempeño del negocio, como por ejemplo, estudios de mercado encargados a empresas terceras con el fin de conocer el posicionamiento de la marca, conocer a la competencia principalmente en los aspectos económicos, nichos de mercado, así como evaluar las nuevas tendencias en el público objetivo. En cuanto a la normativa legal, la Entidad principalmente trabaja con las normas emitidas por el Ministerio de Trabajo y el Ministerio de Educación. En el caso de las fuentes internas, la información es obtenida de los sistemas informáticos *PeopleSoft (BackOffice) y Campus Solution* (Procesos *Core*) para la toma de decisiones.	2
13.3	**Procesa datos relevantes y los transforma en información**	No se han definido procedimientos para el procesamiento integrado de información, así como tampoco se ha definido en qué medida las tecnologías vigentes de la Entidad dan soporte al procesamiento de información, ni en qué medida a nivel de accesibilidad y velocidad de respuestas deberán ser procesador para el usuario final.	1
13.4	**Mantiene la calidad a lo largo de todo el proceso**	La Entidad no ha definido los niveles de revisión de la información que se genera dentro de cada proceso. Así como tampoco cuenta con una política de gestión, calidad y gobierno de información que establezca la obligación de los miembros de la Entidad de verificar que la información que ellos generan y los datos que se exponen ante un tercero (interno o externo) son acordes con la realidad. Tampoco se ha definido la política sobre la gestión física de los datos, almacenamiento y nivel de seguridad así como no se han identificado los niveles de acceso a los empleados según el nivel de criticidad de la información. La Gerencia General, como parte de sus funciones, se encarga de cuidar que toda la comunicación que sale de la entidad cumpla con el tono adecuado y apropiado.	1
13.5	**Evalúa costos y beneficios**	La Entidad no ha evaluado el costo beneficio de la naturaleza, cantidad y precisión de la información. La Entidad ha optado por no activar los log de información a partir de la implementación del nuevo ERP (*People Soft*); sin embargo, esta decisión no recibe el soporte de un análisis de costo beneficio respecto a la información que pudiese obtener estos y a la capacidad requerida en cuanto al volumen de datos que se deben mantener y tampoco se ha considerado el impacto negativo de la modificación o pérdida de información sensible de la Entidad.	1

Principio 14: La Organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del Sistema de Control Interno.			
N°	**Enfoque**	**Comentario**	**P**
14.1	**Comunica la información de control interno**	La Entidad no cuenta con un procedimiento formal para comunicar a todo el personal respecto al Control Interno, los objetivos, importancia, relevancia y beneficios de tener un adecuado Sistema de Control Interno. Por otro lado, en los procesos en los que se encuentran documentadas las actividades no define claramente las personas encargadas de ejecutar los controles en los procesos. Como una buena práctica, la Gerencia General realiza desayunos mensuales a todo nivel de la Entidad con el objetivo de transmitir un mensaje claro con respecto a la importancia del Control Interno desde la visión de la Alta Dirección; sin embargo, es importante considerar que esta práctica tiene un alcance parcial, considerando el número de empleados de la Entidad a nivel nacional. Como se indicó en puntos anteriores, si bien se han comunicado los objetivos a nivel operativo y de cumplimiento, no se han identificado los objetivos del Sistemas de Control Interno y las responsabilidades del personal con relación a ellos. Con respecto al comportamiento y accionar del personal se ha difundido el Código de Conducta que tiene como propositivo comunicar los principios y compromisos éticos primordiales en el cumplimiento de sus actividades y en la toma de decisiones. Tampoco se ha definido qué información será de conocimiento público con respecto a las desviaciones de control identificados.	1
14.2	**Se comunica con el Directorio**	Trimestralmente, se reúne el Comité de Auditoría en el que se expone la eficacia del Sistema de Control Interno y gestión de riesgos a nivel entidad, a través de los resultados de las auditorías y el avance de los planes de acción aparte de otras actividades de cumplimiento vinculadas a la naturaleza de las operaciones de la Entidad.	3
14.3	**Facilita líneas de comunicación independientes**	La Entidad con la finalidad de fortalecer la cultura de confianza y mejorar la eficiencia de su gestión ha implementado el "Canal de Gestión Ética" como una herramienta que sirve para comunicar anónimamente cualquier preocupación seria y sensible relacionada con potenciales irregularidades e incumplimientos del Código de Conducta de la Entidad. Sin embargo, esta herramienta será utilizada a nivel nacional por los alumnos y por los proveedores en el periodo 2015. La Entidad no ha definido formalmente medios alternativos para la comunicación con la Dirección.	2
14.4	**Define el método de comunicación relevante**	La Entidad cuenta con los siguientes canales de comunicación para permitir que la información fluya de manera clara, ordenada y oportuna: 1. Mailing, 2. Portal WEB y 3 Reuniones informativas Si bien se cuenta con ciertos mecanismos de comunicación, tanto interna como externa, no se ha establecido una política que determine los medios de comunicación internos y externos más favorables en términos de estandarización y efectividad.	2

Principio 15: La Organización comunica a las partes interesadas externas los aspectos clave que afectan al funcionamiento del control interno.			
N°	**Enfoque**	**Comentario**	**P**
15.1	**Se comunica con las partes interesadas externas**	La información que se reporta o comunica hacia terceros y entes reguladores, entre otros, pasa por niveles de revisión a nivel operativo y de la Alta Gerencia antes de ser divulgada. La Alta Dirección quien se encargada de dirigir y evaluar las actividades de prensa, comunicación, así como del contenido de las publicaciones y de mantener la buena imagen de la Entidad. Es importante mencionar, en algunos casos la Alta Dirección es asesorada por funcionarios internos y externos, como por ejemplo, en el caso de aspectos comerciales se realiza con el apoyo del área de Comunicaciones de la Entidad y para comunicaciones legales y tributarias se asesora con los abogado externos Estudio Payet, Rey, Cauvi y Pérez Abogados, para la información contable se cuenta con el asesoramiento de la firma PWC, entre otros. Adicionalmente, la Entidad ha publicado a través de su página Web el "Código de Conducta", el cual está dirigido a todo el personal que labora y al alumnado, así como a los proveedores vigentes.	3
15.2	**Permite la recepción de comunicaciones**	La Entidad ha contratado consultores externos para obtener mayor información y de una forma objetiva sobre el funcionamiento del Sistema de Control Interno: - Estudio Payet, Rey, Cauvi y Pérez Abogados en referencia a cualquier tipo de consulta legal como tributaria, promulgación de nuevas leyes, principalmente del Ministerio de Educación y Ministerio de Trabajo, entre otros. - EY en relación con el asesoramiento en la gestión de riesgos y *cosourcing* de auditoría interna - PWC respecto a la auditoría financiera de los estados financieros y la evaluación independiente de la efectividad del control interno Respecto a la retroalimentación procedente de los clientes (alumnos) sobre la calidad de las clases, costo de las pensiones, reclamos, enseñanza de los docentes, entre otros, la Gerencia Comercial es la encargada de recibir, analizar e informar a la Alta Dirección dicho *feedback* ,utilizando como herramientas la página Web de la Entidad, las redes sociales, el *call center* y el libro de reclamaciones. En el caso de retroalimentación de actividades fraudulentas por parte de los clientes y proveedores, el área de Auditoría Interna tiene el encargo de monitorear el Canal de Ética.	3

15.3	**Se comunica con el Directorio**	El resultado de las evaluaciones realizadas por un consultor externo es expuesto al Directorio siempre y cuando se tome en cuenta la importancia del objetivo de la consultoría, criticidad del proceso evaluado así como el costo de la contratación. Sin embargo, estos criterios no se han definido formalmente en políticas y procedimientos tanto para la Alta Dirección como para el Directorio. El resultado de los servicios tercerizados en el enfoque anterior 15.2 son expuestos y comunicados oportunamente al Directorio mencionando las debilidades identificadas en los procesos evaluados así como los planes de acción a realizar con la finalidad de que el Directorio ejecute su responsabilidad de supervisión.	3
15.4	**Facilita líneas de comunicación independientes**	La Entidad con la finalidad de fortalecer la cultura de confianza y la mejora de la eficiencia de su gestión ha implementado el "Canal de Gestión Ética" como una herramienta que sirve para comunicar anónimamente cualquier preocupación seria y sensible relacionada con potenciales irregularidades e incumplimientos del Código de Conducta. Para el año 2015 esta herramienta podrá ser utilizada por el alumnado a nivel nacional y por los proveedores.	3
15.5	**Define el método de comunicación pertinente**	La Alta Dirección no ha definido formalmente (en un documento) los diversos métodos de comunicación que maneja y según el público objetivo, el tipo de comunicación, tiempo de respuesta y requisitos legales o regulatorios. Se observa que la Entidad cuenta con diversos métodos de comunicación como Portal Web, correo electrónico del personal administrativo, docente y alumnado, redes sociales y en caso fuere necesario, notas de prensa a nivel entidad o a nivel agremiación (Asiste Perú).	2
COMPONENTE: ACTIVIDADES DE SURPEVISIÓN			
Principio 16: La Organización selecciona, desarrolla y realiza evaluaciones continuas o independientes para determinar si los componentes del Sistema de Control Interno están presentes y en funcionamiento.			
N°	**Enfoque**	**Comentario**	**P**
16.1	**Tiene en cuenta un mix o combinación de evaluaciones continuas e independientes**	La Entidad cuenta con una combinación de evaluaciones independientes, las que son llevadas a cabo por la Gerencia de Auditoría Interna, y por la consultora a cargo de las revisiones definidas según el Plan de Auditoría. La Gerencia de Auditoría Interna, define cada año las evaluaciones y revisiones que serán consideradas como parte del plan de trabajo del área de Auditoría Interna, las mismas que son revisadas con la Gerencia General. Sin embargo, se identificó que no se cuenta con una metodología definida para la identificación del nivel de madurez del Sistema de Control Interno	3
16.2	**Tiene en cuenta el ritmo de cambios**		
16.3	**Establece referencias para las evaluaciones**	El Comité de Auditoría, sobre la base de la evaluación de riesgos realizada previamente, define el alcance del Plan de Auditoría así como los recursos a utilizar para la ejecución del mismo. Actualmente, ha definido contratar a un consultor externo con la finalidad de que apoye a la evaluación del Sistema de Control Interno a nivel de procesos y reporte junto con el área de Auditoría Interna el resultado de las evaluaciones. Sin embargo, como se mencionó en el punto 7.1 sobre los riesgos operacionales, no se cuenta con un inventario de riesgos por proceso; sin embargo, se revisan y evalúan aquellos riesgos inherentes con calificación moderada, alta y extrema por aquellos procesos con priorización alta.	2
16.4	**Emplea personal capacitado**	El área de Auditoría Interna cuenta con personal capacitado para realizar el monitoreo del cumplimiento de los controles diseñados por las gerencias respectivas. Así mismo, evalúa la presencia y correcto funcionamiento de los componentes del control interno y los resultados de las evaluaciones. Sin embargo, como se comentó en el punto 12.5, se observa que dentro de los integrantes ninguno cuenta con alguna certificación internacional que respalde el conocimiento, las habilidades y las destrezas del auditor interno sobre la práctica de la actividad de auditoría interna.	3
16.5	**Se integra con los procesos del negocio**	Como parte del Plan de Trabajo de Auditoría Interna se han aplicado evaluaciones continuas tomando en consideración los factores críticos identificados en las evaluaciones pasadas. Mensualmente ejecuta ciertas actividades con la finalidad de encontrar incumplimientos o desviaciones a la ejecución de procedimientos, como por ejemplo, la revisión de las horas dictadas por docentes, el pago a proveedores, la revisión de la conciliación bancaria ejecutada por el Contador o la marcación de docentes, entre otros. El resultado de estas evaluaciones son presentadas a la Alta Dirección y a los dueños de los procesos evaluados en el caso de ocurrir alguna desviación con el fin de obtener los planes de acción al respecto. Trimestralmente se presenta al Comité de Auditoría el resultado de dichas evaluaciones así como los comentarios obtenidos por las áreas responsables.	3
16.6	**Ajusta el alcance y la frecuencia**	El Comité de Auditoría define el número de procesos a evaluar durante el año y, asimismo, indica los procesos que deben tener evaluaciones con mayor frecuencia por parte del área de Auditoría Interna, estas decisiones se toman en base a un enfoque de riesgos. En el caso de que la Auditoría Interna no cumpla con el Plan de Auditoría o informe que no sea posible ejecutarlo al 100%, debe exponer los motivos por los cuales no se cumple el objetivo al Comité de Auditoría quien definirá si es necesario disminuir el alcance del plan o brindar mayores recursos al área, como por ejemplo, el uso de proveedores	3

		de servicios externalizados.	
16.7	**Evalúa de forma objetiva**	El área de Auditoría Interna anualmente elabora el Plan de Auditoría, el cual es aprobado por el Comité de Auditoría. Así mismo, dicho plan es elaborado basado en los riesgos y criterios de la Gerencia como procesos previamente evaluados, encargos del Comité y cambios de procesos, entre otros. El resultado de estas evaluaciones es presentado a los dueños del proceso evaluado, a la Alta Dirección y al Comité a fin de que se indiquen las decisiones sobre las recomendaciones incluidas en los informes de cada evaluación. Anualmente, los Estados Financieros de la Entidad son auditados por un auditor independiente emitiendo un dictamen de auditoría referido a la razonabilidad de los saldos de los Estados Financieros. Sin embargo, no se han evidenciado autoevaluaciones realizadas por la Alta Dirección sobre la presencia y el funcionamiento de los componentes del control interno sobre sus propias actividades.	2
Principio 17: La Organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la Alta Dirección y el Directorio, según corresponda.			
N°	**Enfoque**	**Comentario**	**P**
17.1	**Evalúa los resultados**	Las deficiencias del control interno identificadas en las evaluaciones realizadas por el área de Auditoría Interna o el consultor externo son revisadas por el Comité de Auditoría, la Gerencia General y los dueños del proceso evaluado y definen planes de acción con el objetivo de subsanar las deficiencias encontradas. El área de Auditoría Interna es la responsable de realizar el seguimiento a la implementación oportuna de dichos planes. Trimestralmente, la Gerencia de Auditoría Interna presenta el avance de los planes de acción implementados, en proceso y vencidos al Comité de Directorio. El Comité tiene la potestad de decidir si los planes de acción propuestos por las áreas auditadas deben ser complementados o desestimados. La Entidad no ha definido formalmente actividades de supervisión relacionadas con las evaluaciones continuas respecto a las actividades de gestión y supervisión diaria de los empleados con el objetivo de obtener información de las deficiencias en tiempo real y permitan identificar deficiencias con mayor rapidez.	3
17.2	**Comunica las deficiencias**		
17.3	**Controla las medidas correctivas**		

Fuente: Herramienta de elaboración propia en función de la Herramienta Ilustrativa para Evaluar la Efectividad de un Sistema de Control Interno - COSO 2013

Nota bibliográfica

Guadalupe Nataly Urbina Lozada

Nació en Lima, el 10 de marzo de 1985. Bachiller en Ingeniera Industrial, egresada de la Pontificia Universidad Católica del Perú. Guadalupe es Senior de la División de Advisory Services (AS) de la oficina de EY en Lima, con más de 9 años de experiencia en asesoría de negocios, especializándose en control interno, auditoría interna, gestión integral de riesgos, autoevaluación de riesgos, diseño y pruebas de control, SOX, evaluaciones de cumplimiento de riesgo regulatorio (operacional, de mercado y liquidez), rediseño y mejora de procesos, e implementación de SAP, entre otros temas.

John Erick Espinola Arteaga

Nació en Lima, el 7 de junio de 1987. Contador Público Colegiado de la Universidad Nacional Mayor de San Marcos. Cuenta con un Diplomado en Normas Internacionales de Información Financiera (IFRS) de la Universidad ESAN. John es Senior de la división de Advisory Services (AS) de la oficina de EY en Lima, con más de 6 años de experiencia en asesoría de negocios, especializándose en control interno, auditoría interna, SOX, autoevaluación de riesgos, diseño y pruebas de control.