ARTICULO CIENTÍFICO
AUDITORIA DE SISTEMAS BASADA EN RIESGOS AL SNNA DE LA SENESCYT

Christian Vaca; Edison Casanova
patos_nice@hotmail.com, egcasanova@hotmail.com

Universidad de las Fuerzas Armadas – ESPE
Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
Sangolquí, Ecuador
Abril - 2014

Resumen: El ingreso a las Universidades Públicas del Ecuador, se realiza mediante el Sistema Nacional de Nivelación y Admisión (SNNA) que es administrado financiera y operativamente por la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT). Los procesos de admisión y nivelación han operado normalmente sin que exista una evaluación o auditoria a las aplicaciones que los soportan, situación que incrementa los riesgos a los que cada proceso y actividades están expuestas. Por ello, la finalidad de esta investigación fue: relevar y entender los procesos tecnológicos, identificar los riesgos más significativos por medio de una valoración aplicando como marco de referencia las metodologías COSO ERM y COBIT 4.1, así como realizar la evaluación de dichos procesos con el objetivo de establecer recomendaciones que permitan mejorar los controles o deficiencias encontradas y comunicarlas formalmente a los Directivos de la SENESCYT mediante la entrega del Informe de Auditoría. Cumpliendo con buenas prácticas internacionales y locales (NAGAS, NIA, NEA) para el desarrollo adecuado de una Auditoría. El desarrollo práctico de la tesis se ejecutó bajo tres fases: i) Planificación (Relevamiento y valoración de riesgos), ii) Ejecución (Evaluación de Controles y Pruebas Sustantivas) y iii) Elaboración de Informe de Auditoria (Comunicación de resultados). El informe de auditoría con la finalidad de cuantificar cuantitativamente y cualitativamente el estado del proceso establece una opinión que califica el nivel de riesgo que genera el proceso, sea por incumplimiento, falta o inadecuada aplicación de un control, a partir de esta opinión se ha calificado el nivel de madurez del SNNA.

Palabras claves: Educación Superior, COBIT, COSO ERM, SNNA, SENESCYT.

Abstract: The admission to Ecuadorian public universities is performed by the Sistema Nacional de Nivelación y Admisión (SNNA). It is financially and operationally managed by the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT). The admission and leveling processes have operated normally without any assessment or audit by applications that support them, this situation increases the risks to each process and activity is exposed. Therefore, the purpose of this investigation was relieve and understand the technological processes , identify the most significant risks through a risk assessment applying framework methodologies like COSO ERM and

COBIT 4.1. The evaluation of these processes have allowed establish recommendations to improve controls or deficiencies and communicate formally to the SENESCYT executives by delivering the Audit Report. According to international and local best practices (NAGAS , NIA, NEA) for the proper development of an audit , the practical development of the thesis was made under three phases: i) Planning (Survey and risk assessment) , ii) Implementation (evaluation Controls and Substantive Tests) and iii) Preparation of Audit Report (Communication of results). The audit report in order to quantify quantitatively and qualitatively the state of the process establishes a review that rates the level of risk generated by the process , whether for failure, partial compliance or improper application of a control, since this review is rated maturity level of SNNA process.

Key words: University Education, COBIT, COSO ERM, SNNA, SENESCYT.

I. Introducción

La Gestión de la información dentro de las instituciones, ha generado flujos importantes de datos que requieren de tratamiento especial para mantener su integridad, confidencialidad y disponibilidad. Los sistemas informáticos, a la vez que permiten mejorar significativamente la gestión de la información, también ha generado preocupaciones ante su vulnerabilidad, y es por ello que se han requerido cada vez controles más específicos y especializados que ayuden a cumplir y mantener las características de la información.

La mejora va ligada a la revisión y evaluación, es imposible mejorar algo de lo cual se desconoce su estado actual. La Auditoría es un examen objetivo e independiente, que permite entre otras cosas, conocer la madurez de los procesos para determinar las debilidades y proponer mejoras que mitiguen los riesgos asociados.

COBIT 4.1 y COSO – ERM, son metodologías aceptadas mundialmente para gestionar gobiernos TI y gestión de riesgos respectivamente, las mismas que han sido probadas su validez, eficiencia y eficacia; por lo tanto su aplicación ayuda a establecer situaciones de mejora de una manera fácil y con la seguridad de obtener los resultados esperados.

La figura 1, muestra el cubo de COBIT, que indica los procesos de TI, encargados de manejar los recursos de TI, para satisfacer los requerimientos de Negocio.

COBIT 4.1 – (*Control Objetive For Information and Releated Technology* – Objetivos de Control para la Información y Tecnologías Relacionadas), es un marco de trabajo de dominios y procesos desarrollado por ISACA, que contiene las mejores prácticas enfocadas al control para optimizar las inversiones de TI.

La figura 2, muestra la estructura de COBIT 4.1, formada por 4 dominios (PO: Planear y Organizar; AI: Adquirir e Implementar; DS: Entrega y Soporte; y, ME: Monitorear y

Evaluar). Cada dominio tiene sus propios objetivos de control, 34 en total distribuidos así: (PO = 10; AI = 7; DS = 13; ME = 4)

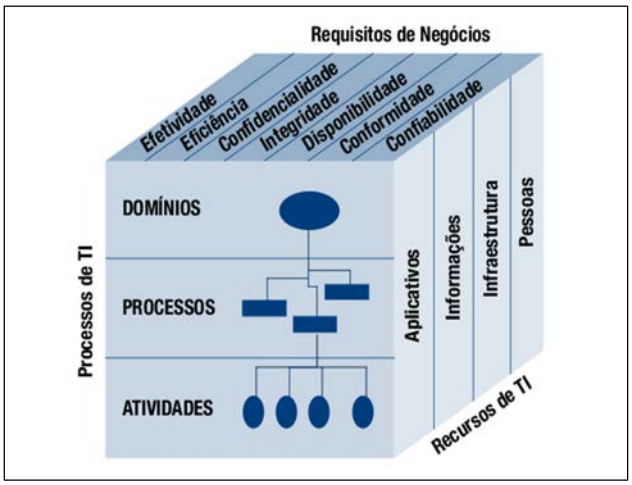

Figura 1. Cubo de COBIT 4.1
Fuente: http://www.joww.net/blog/wpcontent/uploads/2010/10/CuboCobit.png

Figura 2. Estructura COBIT
Fuente: COBIT 4.1

COSO ERM – (*Committee Of Sponsoring Organization Of The Tread Way Commission, Enterprise Risk Management* – Comité de Organizaciones Patrocinadoras, Administración del Riesgo Empresarial), es una buena práctica que logra definir un marco conceptual común y se constituye en una visión integradora del control interno mediante la administración de los riesgos empresariales.

La figura 3, muestra el cubo COSO – ERM, el cual contiene los objetivos institucionales clasificados en cuatro categorías (parte superior del cubo), ocho elementos propios de la metodología (parte frontal del cubo) y de alcance corporativo considerando las actividades de todos los niveles de la organización (parte lateral del cubo).

Figura 3. Cubo COSO – ERM
Fuente: http://www.mapfre.com/fundacion/html/revistas/gerencia/n098/img/fotos/m53_7.jpg

COSO – ERM describe un marco basado en principios, el mismo que provee: definición de administración de riesgos corporativos; principios críticos y componentes de un proceso de administración de riesgos corporativos efectivo; Pautas para las organizaciones sobre cómo mejorar su administración de riesgos; y, Criterios para determinar si la administración de riesgos es efectiva, y si no lo es que se necesita para que lo sea.

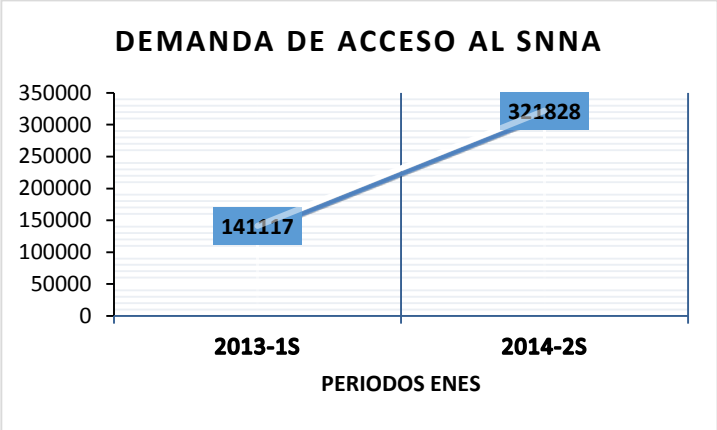

Figura 4. Crecimiento de la demanda de acceso al SNNA
Fuente: SENESCYT

La aprobación del Constitución de la República en el 2008, y de la LOES en el 2010, establecen los principios en los que se regirá la política pública de Educación Superior en el Ecuador, entre estos aspectos se encuentra el Sistema Nacional de Nivelación y Admisión - SNNA, que tiene como propósito garantizar un acceso al sistema de Educación Superior aplicando el principio de justicia y considerando las áreas estratégicas que aportan al cumplimiento del Plan Nacional del Buen Vivir y al cambio de la matriz productiva.

La figura 4, muestra la creciente demanda que ha sufrido el acceso a la Educación Superior desde la aplicación del primer Examen Nacional de Educación Superior – ENES, hasta la actualidad.

Debido a la cantidad de información que genera el SNNA, se ha implementado sistemas informáticos para automatizar y gestionar la información de una manera efectiva. Para automatizar el proceso de Admisión se genera un convenio con el Centro de Transferencia Tecnológica de la Universidad de las Fuerzas Armadas – ESPE y para el proceso de Nivelación se alquila la plataforma Universitas XXI de la Oficina de Cooperación Universitaria – OCU. Estas soluciones informáticas, no han atravesado por un examen de evaluación que permita determinar sus fortalezas y debilidades, para en base a ello establecer adecuadamente un Gobierno de TI que integre e institucionalice mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicio y soporte y monitoreo y evaluación de los servicios de TI, para asegurar que la información del SNNA y las tecnologías relacionadas soporten los objetivos de la SENESCYT.

La evaluación y la auditoría son procesos necesarios para establecer recomendaciones y controles útiles para el mejoramiento de los procesos SNNA. Esta investigación se realizó considerando los procesos de admisión y nivelación de los períodos 2013-1S y 2013-2S, para entregar como resultado final un informe de auditoría que contiene recomendaciones

y controles cuya implementación y aplicación queda a criterio y responsabilidad de las autoridades de la SENESCYT.

Gestión de Riesgos, Auditoría basada en Riesgos y Modelo de Madurez CMMI

Kincaid James, en la guía de estudio para el examen de certificación en autoevaluación de control – CCSA, define al riesgo como: "El riesgo es la probabilidad de que ocurra un evento que pueda tener un impacto en el alcance de los objetivos. El riesgo se mide en términos de consecuencias y probabilidad de que este ocurra." (JAMES, 2008)

Los riesgos afectan al logro de los objetivos de las organizaciones, por lo tanto bajo Gestión de Riesgos se los puede categorizar como, Riesgos Estratégicos, Operacionales, de Reportes y de Cumplimiento.

El autor de la obra "Risk - Based Auditing" (Phil Griffiths), define a la auditoría basada en riesgos como: "un proceso, un acercamiento, una metodología y una actitud en torno al tema. La manera más simple de definir una auditoría basada en riesgos consiste en revisar las cosas que realmente importan en su organización" (GRIFFITHS, 2005)

Un examen de auditoría, requiere un enfoque que permita identificar y mitigar los riesgos asociados a los procesos a evaluar por medio de la identificación de controles y aplicación de pruebas sustantivas, para ello existen varias metodologías, En La figura 5, se detalla el esquema básico para el desarrollo de una auditoría.

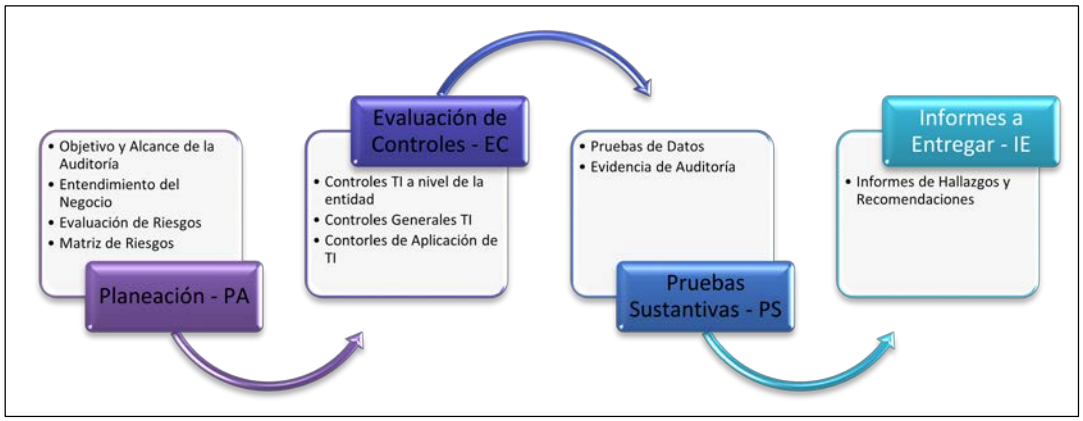

Figura 5. Fases de la Auditoría
Fuente: Propia

El Modelo Integrado de Capacidad y Madurez (CMMI), es un modelo alineado con COBIT 4.1 para la mejora y evaluación de los procesos de desarrollo y mantenimiento de sistemas y productos de software de una empresa, que propone un esquema de cinco niveles de madurez detallados en la figura 6.

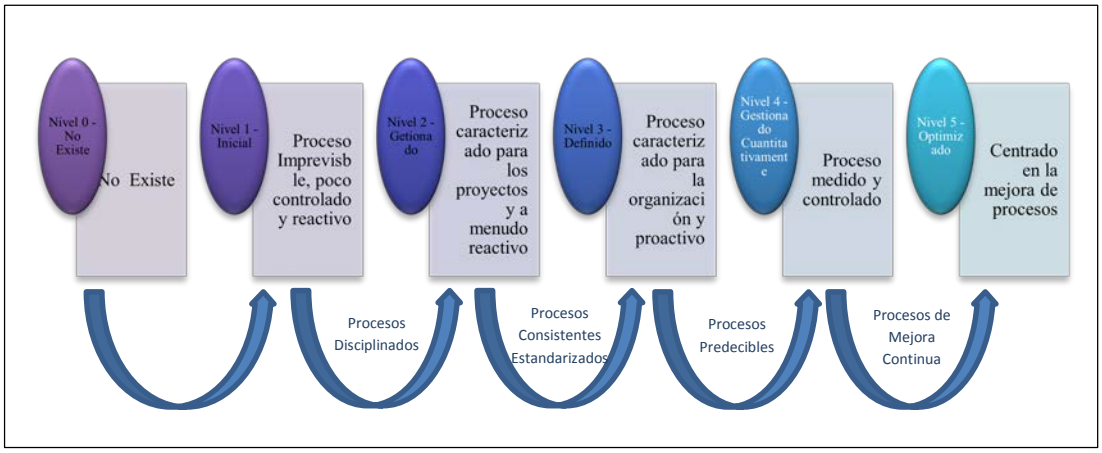

Figura 6. CMMI – Niveles de Madurez
Fuente. CMMI

II. Metodología

La presente investigación es de naturaleza cualitativa, ya que se utilizó registros narrativos de los fenómenos estudiados mediante técnicas de observación e indagación.
En la evaluación de la situación actual se utilizó el método deductivo. Previo análisis y síntesis se obtuvo premisas que determinan la realidad institucional plasmada en el desarrollo de los procesos

La revisión literaria también fue fundamental en la investigación. Se levantó información recolectada en la institución por medio de solicitud y la observación directa, así como también de los documentos que aportan significativamente al tema, que no necesariamente pertenecen a la SENESCYT, sino que son producto de investigaciones relacionadas. Se realizó el respectivo registro de esta documentación en los papeles de trabajo de la auditoria conocido como recorrido del proceso.

En la investigación se ha establecido el grado de madurez de los procesos tecnológicos en relación al nivel de confianza calculado. Sin embargo, considerando que los resultados de la auditoría pretenden ser un aporte para fortalecer los procesos de TI y buscar su adecuada alineación con los objetivos institucionales sin importar el estado de madurez actual de los procesos TI, el nivel de madurez no es un factor preponderante en los resultados de la investigación. Cobit 4.1, expresa acerca de los modelos de madurez: “El propósito no es avaluar el nivel de adherencia a los objetivos de control. Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser

usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.” (IT GOBERNANCE INSTITUTE, 2007)

Para elaborar la matriz de riesgos se utilizó la metodología COSO ERM y COBIT 4.1, para lo cual fue necesaria la inclusión de técnicas de recolección de información, que permitieron mantener un orden establecido y generar datos significativos para la investigación, guardando estrecha relación del tema con las buenas prácticas usadas tanto para análisis de riesgos como para definir los procedimientos de la auditoría.

Las ponderaciones de los riesgos fueron revisadas y validadas con la SENESCYT, considerando que es la alta gerencia la responsable de definir y gestionar sus riesgos, según buenas prácticas de gestión de riesgos.

Para calcular la muestra, se utilizó la fórmula para poblaciones finitas mostrada en la Ecuación 1, puesto que la población de postulantes cumple con esta característica.

Ecuación 1. Cálculo de muestras finitas

$$m = \frac{K^2 Npq}{e^2(N-1) + K^2 pq}$$

Una vez calculada la muestra, se elaboró una macro que selecciona aleatoriamente datos de nuestro universo, considerando como parámetro de estratificación la distribución equitativa de postulantes por periodo, que para el caso representa aproximadamente 50% para cada período evaluado. Para conocer el significado de cada término de la Ecuación 1, el código fuente de la macro y la forma como esta estratifica la muestra, refiérase al documento de la tesis (página 103).

III. Evaluación de resultados y discusión

La evaluación de los controles se realizó mediante la valoración de la condición y el criterio, se comparó estos dos parámetros, es decir, "lo que es" con "lo que debe ser" respectivamente, y se marcó los controles de acuerdo al cumplimiento de los eventos detallados en el cuadro 2.

Se sumó el número de repeticiones por evento para obtener el total de cada uno de ellos (TE), se restó del total de eventos válidos (VV) el total de eventos no aplica (NA), y se calculó el porcentaje (PR) que este valor representa en relación al total. Para obtener el grado de confianza (GC), se multiplicó el porcentaje PR por la ponderación máxima establecida (5); para calcular el grado de riesgo (GR), se resta del valor máximo de riesgo

(5) el valor del grado de confianza GC; este valor promediado con ajuste de riesgo (AR), resulta el valor del riesgo total (RT). Para una explicación detallada del esquema utilizado para valoración de riesgos, refiérase al documento de la tesis (página 105).

Cuadro 1
Calificación Condición - Criterio

Marca de Auditoría a Utilizar	Equivalencia	Control - Evento a Verificar
✓	Si	Es conforme, cuando se ajusta satisfactoriamente a los criterios
✗	No	No cumple, cuando no se ajusta a los criterios
✗	No	No cumple, cuando se ajusta parcialmente a los criterios
✓	Si	Es conforme, cuando supera los criterios
⊘	No aplica	La condición no aplica para el control o evento evaluado

Fuente: Propia

El esquema indicado fue aplicado a los dos subprocesos (admisión y nivelación), y considerando cada prueba de control y de detalle, de esta forma se obtuvo un valor de riesgo por subproceso (Ver cuadro 3).

Cuadro 2
Resumen de Evaluación de Riesgos - SNNA

RIESGO TOTAL		
PROCESO	**RIESGO**	**VALOR**
Admisión	Moderado	3,96
Nivelación	Moderado	3,84
RIESGO SNNA	**Moderado**	**3,90**

Fuente: Propia

Finalmente se establece el riesgo total del SNNA con un valor de 3,90 (Ver cuadro 3), que resulta de promediar los valores individuales de cada subproceso. Este valor de riesgo permitió establecer la opinión de auditoría que se indica en el cuadro 4, dicha opinión es resultado de aplicar las ponderaciones acordadas con la SENESCYT. Para una explicación detallada del cuadro de ponderaciones, refiérase al documento de la tesis (página 110).

IV. Trabajos Relacionados

La SENESCYT, es una institución relativamente nueva que nace con la aprobación de Ley Orgánica de Educación Superior, esta institución es la implementadora del SNNA, que se constituye en un único Sistema de Admisión y Nivelación a nivel Nacional reportado en la historia del Ecuador, y si bien es cierto que ciertas Instituciones de Educación Superior – IES, han implementado procesos de admisión, ninguno de ellos ha tenido las características del SNNA de la SENESCYT.

La presente investigación no tiene antecedentes, es la primera vez que los sistemas informáticos del SNNA se someten a un examen de auditoría.

No se relaciona el presente trabajo con otros de nivel internacional, porque el hecho de tener un sistema de Nivelación y Admisión que considera inclusive la brecha actual entre el bachillerato y la Educación Superior, lo constituye un proceso nuevo y único que busca acoplarse con medida exacta a las necesidades institucionales, las mismas que responden a las necesidades de una población única a nivel mundial.

Cuadro 3
Opinión de Auditoría

Calificación Riesgo:	Moderado	**Madurez del Control:**	Se requiere una mejora importante
Opinión:			
Se han identificado numerosas debilidades concretas en los controles. Los controles evaluados probablemente no podrían proporcionar una garantía razonable de que los riesgos están siendo gestionados y que se lograrán los objetivos			

Fuente: Propia

V. Conclusiones y trabajo futuro

La valoración de riesgos y el análisis de controles con el uso de COSO – ERM y COBIT 4.1, ha permitido recomendar situaciones específicas que garantizan un gobernanza TI alineada a los objetivos estratégicos de la SENESCYT para el cumplimiento de los requerimientos del SNNA.

El Reglamento a la Ley de Transparencia y acceso a la información pública, que establece en el capítulo III – Art. 9: "…, en los términos de la legislación vigente, se considera reservada la información, cuando se trate de: …; c) Información de auditorías y exámenes especiales programadas o en proceso." (ASAMBLEA NACIONAL, 2013).

Se concluye con un informe de auditoría donde constan los hallazgos y recomendaciones, que en cumplimiento a lo especificado en el párrafo anterior, se entrega con carácter de "Confidencial" únicamente a la SENESCYT, y se lo excluye del informe final de tesis, el mismo que contiene el criterio de auditoría como resultado de la investigación.

El informe de auditoría establece situaciones que pueden ser consideradas, si la SENESCYT lo considera pertinente, como tema de futuras investigaciones, en este caso, la presente investigación servirá de sustento preliminar y fundamento científico.

Con base en la presente investigación, se puede realizar un proyecto para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información - SGSI, con el

uso de normas mundialmente aceptadas que garantizan resultados eficientes y eficaces, tal es el caso de la ISO 27002.

Es necesario para la SENESCYT diseñar, implementar, probar y aprobar un Plan de Continuidad del Negocio - BCP, alineado con ITIL, COBIT y la norma ISO 27001, que encaje con el presente trabajo y generen un complemento mutuo de utilidad en la gestión de la información y el Gobierno TI en la Institución.

Referencias Bibliográficas

ASAMBLEA NACIONAL. (2010). *Ley Orgánica de Educación Superior*. Quito.

ASAMBLEA NACIONAL. (2013). *Reglamento a la Ley de Transparencia y Acceso a la Información Pública.* Quito.

ASAMBLEA NACIONAL CONSTITUYENTE. (2008). *Constitución de la República del Ecuador*. Montecristi.

GRIFFITHS, P. (2005). *Risk - Based Auditing.*

IIA. (2005). *GTAG - Controles de Tecnología de la Información.* Florida.

INSTITUTO DE AUDITORES INTERNOS DEL ECUADOR. (2013). *Taller de Mapas de Riesgos Corporativos.* Quito.

ISACA. (s.f.). *Marco de Riesgos de TI.* ISACA.

IT GOBERNANCE INSTITUTE. (2007). *COBIT 4.1*. Estados Unidos.

JAMES, K. (2008). *CCSA - Certificación en Autoevaluación de Control - Guía de Estudio Para el Examen.* Florida: IIARF.

PRICE WATERHOUSE COOPERS. (2005). *Gestión de Riesgos Corporativos Marco Integrado.* New Jersey: AICPA.

SENESCYT. (2013). *Reglamento del Sistema Nacional de Nivelación y Admisión SNNA.* Quito: LEXIS.