VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE MAGISTER

TEMA: EVALUACIÓN TÉCNICA A LA IMPLEMENTACIÓN DE LA FASE I DEL ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CEAACES

AUTORES:
CABRERA TAPIA, CÉSAR ANTONIO
MOREJÓN MARIÑO, JUAN BOLÍVAR

DIRECTOR: ING. RON GAVI, MARIO GIOVANNY

SANGOLQUÍ
2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO DE CUMPLIMIENTO DE LA TESIS.

Sangolquí, 04/05/2015

Señor
Ing. Rubén Arroyo, Mgts
COORDINADOR DE LA MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS
Presente.-

Yo, Ing. Mario Giovanny Ron Gavi, certificó que los mencionados maestrantes los Ings. César Antonio Cabrera Tapia y Juan Bolívar Morejón Mariño, egresados del Programa de Maestría en Evaluación y Auditoria de Sistemas Tecnológicos, VII-A Promoción, ha presentado la tesis Titulada"Evaluación Técnica a la implementación de la Fase I del Esquema Gubernamental de la Seguridad de la Información en el CEAACES", la misma que ha sido revisado en su totalidad en forma y fondo, la cual reúne las condiciones de calidad para ser presentado en la defensa y el empastado entregado a biblioteca, por lo que solicitó se digne disponer el trámite correspondiente.

El presente trabajo es fruto de su investigación, el cual ha sido orientado durante su ejecución por los suscritos.

Atentamente.-

.....
DOCENTE DIRECTOR
Ing. Mario Giovanny Ron Gavi, Mgts

DECLARACIÓN

Nosotros, César Antonio Cabrera Tapia y Juan Bolívar Morejón Mariño, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad de las Fuerzas Armadas ESPE, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

César Antonio Cabrera Tapia

Juan Bolívar Morejón Mariño

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, César Antonio Cabrera Tapia y Juan Bolívar Morejón Mariño Autorizamos a la Universidad de las Fuerzas Armadas ESPE la publicación en la biblioteca virtual de la Institución, menos los anexos que comprometan datos críticos Institucionales, del trabajo “Evaluación Técnica a la implementación de la Fase I del Esquema Gubernamental de la Seguridad de la Información en el CEAACES”, cuyo contenido, ideas y criterios son de nuestra entera exclusiva responsabilidad y autoría.

Atentamente,

César Antonio Cabrera Tapia
CC. 0103080693

Juan Bolívar Morejón Mariño
CC. 1802817468

DEDICATORIA

Dedico este trabajo a las personas que son mi motivo para seguir adelante, que permiten que cada sacrificio se recompense con una gran sonrisa y un fuerte abrazo, mis tías Cecy y Loli, mi esposa Andrea y mi hijo Hernán, que mágicamente logran que todos los días sea muy feliz con lo que soy y lo que hago.

César Cabrera

AGRADECIMIENTO

Quiero agradecer a muchas personas que me han apoyado siempre de forma incondicional: mis padres, mis profesores, mis compañeros, y especialmente a mi compañero, que más que eso es un gran amigo, Juan Morejón y a mi tutor de tesis el Ing. Giovanny Ron, que nos guió con la mejor colaboración y voluntad con su amistad y conocimiento profesional en la elaboración de esta tesis

César Cabrera

DEDICATORIA

Dedico este trabajo a las personas que me han apoyado siempre, mis queridos hijos, a mis padres, a Michelle y sobre todo al Gran Arquitecto del Universo que me permite continuar siendo cada día para ser mejor.

Juan Morejón

AGRADECIMIENTO

A las personas que nos apoyaron para el cumplimiento de este trabajo, a mis profesores, personal de CEAACES, a mi tutor Giovanny Ron, a César Cabrera que sin su apoyo no podría haber concluido esta tesis.

Juan Morejón

RESUMEN

La Secretaría Nacional de Administración Pública, el 19 de septiembre de 2013 publica el Acuerdo 166, en el que consta como documento base la norma ecuatoriana NTE INEN ISO/IEC 27002, que a su vez es una adopción de la norma internacional ISO/IEC 27002, de cumplimiento obligatorio para todas las Instituciones de la Administración Pública Central, dentro de este acuerdo, existen 98 controles definidos como prioritarios con un plazo inicial para el cumplimiento de las mismas hasta el mes de marzo de 2014, a estas 98 controles se enfoca la presente Evaluación Técnica. El objetivo general de este trabajo es evaluar la implementación de la Fase I del Acuerdo 166 en el CEAACES, los objetivos específicos son: evaluar el cumplimiento en las normas y en los plazos, evaluar la eficacia y eficiencia de los controles aplicados y realizar una matriz de análisis de riesgos, y por último priorizar los riesgos informáticos. La metodología de investigación a usar será descriptiva y cualitativa, es decir, se va a diseñar una auditoría, con las fases de planificación, ejecución y entrega de resultados, con las técnicas de investigación de campo, entrevistas, encuestas, evidencia de los hallazgos. En este caso no se hará muestreo ya que se va a revisar el 100% de las normas o disposiciones de la Fase I, debido a que el universo es pequeño y se debe revisar todos los puntos de la Fase I. Este trabajo está dividido en cuatro capítulos que son la introducción, marco teórico, aplicación y ejecución, y conclusiones y recomendaciones.

PALABRAS CLAVES:

SEGURIDAD DE LA INFORMACIÓN

SISTEMAS DE GESTIÓN

AUDITORÍA INFORMÁTICA

FUNDAMENTACIÓN TÉCNICA

EVALUACIÓN DE RIESGOS

SUMMARY

The National Secretariat of Public Administration, on September 19, 2013 published the Agreement Nº 166, which has based on a main document of Ecuadorian standard NTE INEN ISO / IEC 27002, those is like an adoption of the international standard ISO / IEC 27002 , binding on all institutions of the Central Public Administration observance within this agreement, there are 98 controls defined as priority with an initial deadline for compliance with them until the month of March 2014, these 98 controls focuses the Technical Assessment. The general objective of this study is assessing the implementation of Phase I of the Agreement in the CEAACES 166, the specific objectives are: check out compliance to the rules and deadlines, evaluate the efficiency and effectiveness of the controls applied and perform an array risk analysis, and finally prioritize IT risks. The research methodology will be used a descriptive and qualitative, namely, we are going to designing an audit, with the planning, execution and delivery of results, with the techniques of field research, interviews, surveys, evidence of the findings. In this case, it will not be sampling because it´s going to check a 100% of the rules and provisions of Phase I, owing for an universe is small and should be review all points of Phase I. This work is divided into four chapters are the introduction, theoretical framework, implementation and enforcement, and conclusions and recommendations.

Keywords

SYSTEM INFORMATION

MANAGEMENT SECURITY

COMPUTER AUDITING

TECHNICAL FOUNDATION

RISK ASSESSMENT

Contenido Página

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

1.1 Título

Evaluación técnica a la implementación de la Fase I del Esquema Gubernamental de la Seguridad de la Información en el CEAACES.

1.2 Resumen

La Secretaría Nacional de Administración Pública, el 19 de septiembre de 2013 publica el Acuerdo 166, en el que consta como documento base la norma ecuatoriana NTE INEN ISO/IEC 27002, que a su vez es una adopción de la norma internacional ISO/IEC 27002, de cumplimiento obligatorio para todas las Instituciones de la Administración Pública Central, dentro de este acuerdo, existen 98 controles definidos como prioritarios con un plazo inicial para el cumplimiento de las mismas hasta el mes de marzo de 2014, a estas 98 controles se enfoca la presente Evaluación Técnica. (Secretaría Nacional de la Administración Pública, 2013)

El objetivo general de este trabajo es evaluar la implementación de la Fase I del Acuerdo 166 en el CEAACES, los objetivos específicos son: evaluar el cumplimiento en las normas y en los plazos, evaluar la eficacia y eficiencia de los controles aplicados y realizar una matriz de análisis de riesgos, y por último priorizar los riesgos informáticos.

La metodología de investigación a usar será descriptiva y cualitativa, es decir, se va a diseñar una auditoría, con las fases de planificación, ejecución y entrega de resultados, con las técnicas de investigación de campo, entrevistas, encuestas, evidencia de los hallazgos. En este caso no se hará muestreo ya que se va a revisar el 100% de las normas o disposiciones de la Fase I, debido a que el universo es pequeño y se debe revisar todos los puntos de la Fase I.

Este trabajo está dividido en cuatro capítulos que son la introducción, marco teórico, aplicación y ejecución, y conclusiones y recomendaciones.

1.3 Justificación e importancia

Con excepción del Acuerdo 166 realizado por la Secretaría Nacional de la Administración Pública (SNAP), actualmente la única legislación ecuatoriana que obliga a cumplir normativas relacionadas con seguridad de la información, es dada por la Superintendencia de Bancos y Seguros (SBS) que es una institución pública que regula y controla a las instituciones bancarias y compañías de Seguros. Ver Figura 1.

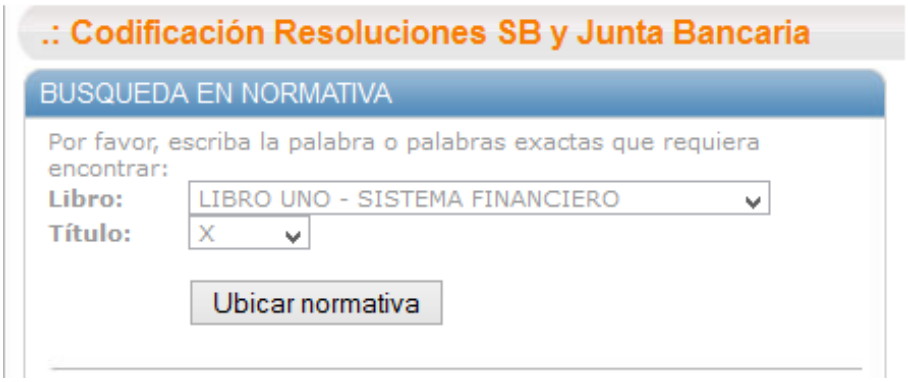

Figura 1 – Página web de la Superintendencia de Bancos y Seguros

En el Libro I de *Sistema Financiero*, Título X *De la Gestión y Control de Riesgos*, Capítulo 5 *De la Gestión del Riesgo Operativo*, se pueden encontrar instrucciones acerca de seguridad de la información en los siguientes numerales: (Superintendencia de Bancos y Seguros, 2014)

- 4.3.5 Medidas de seguridad en Canales Electrónicos,
- 4.3.6 Cajeros automáticos,
- 4.3.7 Puntos de venta (POS y PIN Pad)

- 4.3.8 Banca electrónica,

- 4.3.9 Banca móvil,

- 4.3.10 Sistemas de audio respuestas (IVR),

- 4.3.11 Corresponsales no bancarios

La Sección VII, de este capítulo que se titula “Seguridad de la información” consta de los artículos 21 y 22, que recomiendan la aplicación de la familia de normas ISO/IEC 27000, o alguna parecida que cumpla con los requisitos propuestos, y la implementación de un Sistema de Gestión de Seguridad de la Información.

Sin embargo esta normativa no brinda controles específicos en el tema de la seguridad de la información, sino que da indicaciones muy generales de seguridad en aplicaciones bancarias, sin la alineación de un estándar internacional específico o un código de buena práctica en seguridad de la información.

1.4 Planteamiento del problema

Todas las instituciones de la Administración pública central, institucional y que dependen de la Función Ejecutiva, deben aplicar el aplicación del Acuerdo 166, de cumplimiento obligatorio realizado por la SNAP para implementar el EGSI, tienen un plazo de seis para la implementación de la Fase I y de dieciocho meses para el resto de controles a partir de su expedición que fue en el mes de septiembre de 2013.

El Acuerdo 166 se incluye en el Anexo A, los controles prioritarios se marcan con un asterisco, a ser realizados en la Fase I.

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información. La confidencialidad significa que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. La integridad es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. La disponibilidad es el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO 27000, 2014)

Es necesario evaluar la implementación de la Fase I, que según el Art. 2 del Acuerdo 166 debía estar completado en el mes de marzo de 2014. Sin embargo, no se ha logrado implementar en su totalidad y/o en los plazos programados según el cronograma todos los puntos que se consideran prioritarios, debido que no existe una cultura organizacional y una experiencia previa de las personas que laboran en los niveles directivos, operativos y de apoyo en el sector público en el tema de la seguridad de la información a través de un esquema de mejora continua como se plantea en las normas de la familia ISO 27000 lo que causa que la información de entidades del gobierno se encuentren vulnerables frente a eventos de riesgo.

Es importante realizar un análisis del riesgo que implica el no cumplimiento de cada una de estas disposiciones, mediante una auditoría técnica inicial de los hallazgos de las evidencias encontradas en torno al grado de cumplimiento de estos controles, mediante las mejores prácticas y normativas nacionales e internacionales de la auditoría informática, que han sido implantadas en otros países, en los campos público y privado. Estos hallazgos tendrán dos beneficios claves para la buena marcha de la institución, será información muy valiosa para la retroalimentación del EGSI en el proceso de mejora continua y en el tema de asignar mejor todo tipo de recursos monetarios, humanos, de equipo, que casi siempre son insuficientes.

Por último hay que evaluar la eficacia y eficiencia de estos controles que se obligan a cumplir en el Acuerdo 166, ya que algunos controles por temas técnicos, legales y de otra índole sean inaplicables, ilegales o innecesarios en la Administración Pública.

1.5 Formulación del problema a resolver

- ¿Se ha logrado el cumplimiento de la implementación de la Fase I del Acuerdo 166 en el CEAACES, tanto en las normas o disposiciones, y en la fecha propuesta?

- ¿Los objetivos de control son aplicables de forma eficaz y eficiente?

- ¿Existe una priorización de los objetivos de control basados en un análisis de riesgo, que contenga las variables Impacto - Probabilidad?

1.6 Hipótesis

No aplica

1.7 Objetivo General

- Evaluar el cumplimiento de la implementación de la Fase I del Acuerdo 166 del Esquema Gubernamental de la Seguridad de la Información - EGSI en el CEAACES.

1.8 Objetivos Específicos

- Realizar la planificación, ejecución y entrega de resultados de la evaluación del cumplimiento de la implementación de la Fase I del Acuerdo 166 en el CEAACES y evidenciar los hallazgos.

- Evaluar la eficiencia y eficacia de los objetivos de control.

- Priorizar los objetivos de control mediante un análisis basado en el riesgo.

1.9 Introducción

El objetivo de la SNAP es mejorar la eficiencia de las instituciones del Estado, para lo cual un aspecto importante es tener una normativa unificada para la gestión de la seguridad de la información en todo el Estado, verificando que cada institución cumpla con la implementación de esta normativa en los artículos y plazos propuestos.

1.9.1 Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, (CEAACES)

El CEAACES, es el organismo técnico, público y autónomo encargado de ejercer la rectoría política para la evaluación, acreditación y el aseguramiento de la calidad de las Instituciones de Educación Superior, sus programas y carreras. Para ello, realiza procesos continuos de evaluación y acreditación que evidencien el cumplimiento de las misiones, fines y objetivos de las mismas. (CEAACES, 2014)

Se puede observar en el organigrama del CEAACES que la Unidad de Tecnologías y Comunicación, forma parte de la Coordinación General Administrativa Financiera.

Se encuentra en la ciudad de Quito. Tiene influencia en todo el sector educativo superior en el territorio nacional de la República del Ecuador. Ver la Figura 2.

Provincia:	Pichincha
Cantón:	Quito
Dirección:	Germán Alemán E11 – 32 y Javier Arauz
Coordenadas geográficas:	UTM 17M 780850E 9980125S

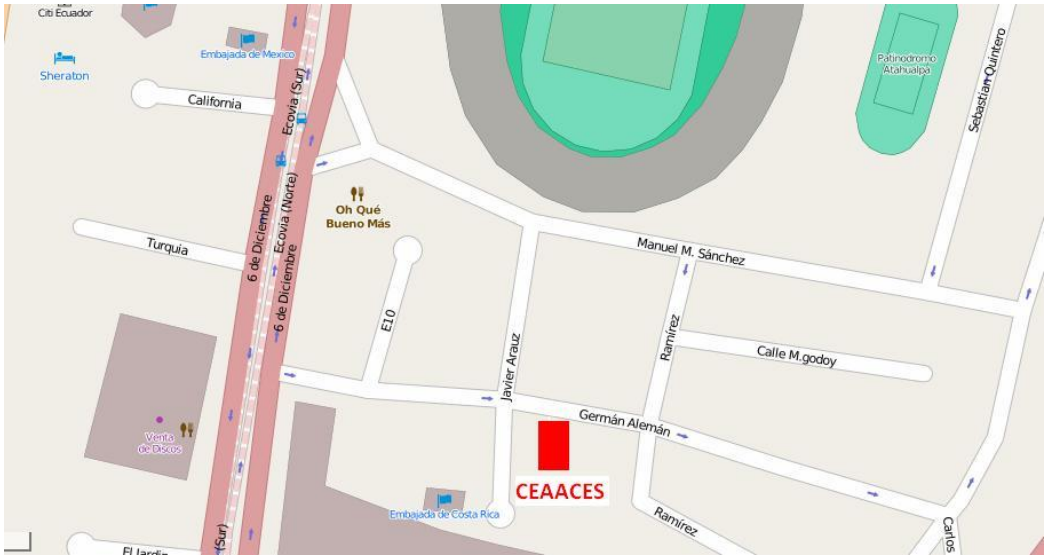

Figura 2 – Ubicación geográfica del CEAACES

Misión y Visión del CEAACES

Misión:

Ejercer la rectoría de la política pública para el aseguramiento de la calidad de la educación superior del Ecuador a través de procesos de evaluación, acreditación y categorización en las IES. (CEAACES, 2014)

Visión:

Ser un referente nacional y regional en la creación e implementación de metodologías integrales, articuladas y transparentes de evaluación, acreditación y aseguramiento de la calidad de la educación superior. (CEAACES, 2014)

1.9.2 Consejo de Educación Superior (CES)

El Consejo de Educación Superior (CES) tiene como su razón de ser planificar, regular y coordinar el Sistema de Educación Superior, y la relación entre sus distintos actores con la Función Ejecutiva y la sociedad ecuatoriana; para así garantizar a toda la ciudadanía una Educación Superior de calidad que contribuya al crecimiento del país. El CES trabajará en coordinación con el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior- CEAACES para continuar con la Revolución en el Conocimiento de una forma integral y profunda. (CES, 2015)

Misión y visión del CES

Misión

El Consejo de Educación Superior, como uno de los dos organismos que rigen el sistema, tiene como misión la planificación, regulación y coordinación interna del Sistema de Educación Superior del Ecuador, y la relación entre sus distintos actores con la Función Ejecutiva y la sociedad ecuatoriana. (CES, 2015)

Visión

Ser el organismo público referente para los procesos que consoliden el Sistema de Educación Superior, ejerciendo sus competencias constitucionales y legales, de forma que incidan decisivamente en el logro de la excelencia de la educación superior mediante la formación académica y profesional, con visión científica y humanística que contribuya con soluciones a los problemas del país articulados al régimen de desarrollo y al del buen vivir; respetando los principios constitucionales que rigen a las Instituciones y al Sistema de Educación Superior. (CES, 2015)

El CES en su constitución manifiesta que trabaja conjuntamente con el CEAACES, para el aseguramiento de la calidad de los Institutos de Educación Superior.

CAPÍTULO II

2.1 Fundamentación teórica

2.1.1 Seguridad de la información

La información es un activo que representa un gran valor dentro de la organización, sea este tangible o intangible, por lo tanto requiere una protección adecuada ya sea por diferentes medios o técnicas de seguridades implantadas. Para estos hay que tomar muy en cuenta el creciente ambiente interconectado de negocios es por esto que la información está expuesta a un mayor rango de amenazas y vulnerabilidades. (Romo & Valarezo, 2015)

El proceso de auditoría de la seguridad de la información se basa en el análisis de los riesgos, entendiéndose el riesgo como efecto de la incertidumbre en los objetivos como se indica en la Guía ISO 73:2009. (ISO 73, 2009)

La seguridad de la información debe ser un proceso de mejora continua, por eso la norma ISO recomienda crear un SGSI, basado en el círculo de Deming, PHVA, (Planificar, Hacer, Verificar, Actuar) o por sus siglas en inglés PDCA (Plan,Do, Check, Act) por lo que se recomienda crear un SGSI dentro de las organizaciones. Este método ha sido implementado con éxito en las empresas y organizaciones mediante los Sistemas de Gestión de Calidad (SGC) y los Sistemas de Gestión de la Seguridad de la Información (SGSI) y es la base del concepto de mejora continua, que se aplica en la familia de normas ISO 9000. Ver Figura 3.

Figura 3 – Círculo de Deming

La seguridad de la información en una normativa empezó con la Institución Británica de Normalización (British Standards Institution BSI) con la norma BS 7799-1:1995 *Information security management. Code of practice for information security management systems* que luego fue adoptado por ISO/IEC como ISO/IEC 17799 *Information technology -- Code of practice for information security management,* y actualmente es la ISO/IEC 27002.

La norma BS 7799-2 se convirtió en ISO/IEC 27001 que es la única norma certificable de la serie de ISO/IEC 27000.

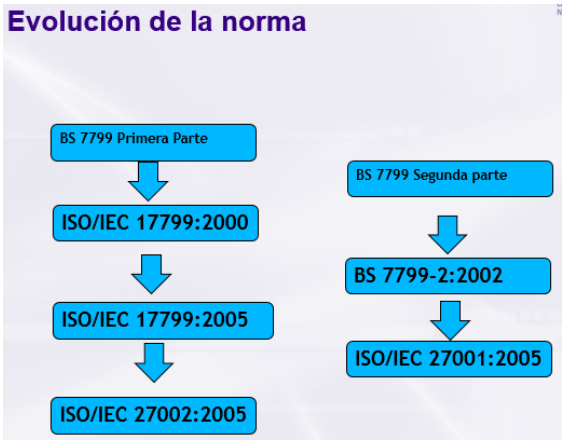

Figura 4 – Evolución de la normativa de seguridad de la información

Los criterios más importantes que se consideran en la Seguridad de la Información son la confidencialidad, integridad y disponibilidad. Otros requisitos a considerar son la autenticidad, no repudio, responsabilidad, fiabilidad.

2.1.2 Mecanismos básicos de seguridad

Autenticación.- Es la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger. (Mifsud, 2015)

Autorización.- Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Administración de TI.- Es la que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Auditoría.- Es la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización. (Mifsud, 2015)

Registro- Es el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo. Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada. Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo. (Mifsud, 2015)

2.1.3 Vulnerabilidad de un sistema de TI

En un sistema de TI lo que se quiere preservar son sus activos que son los recursos como: hardware, software, datos, talento humano y otros.

De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

2.1.4 Políticas de seguridad de la información

Lo primero que se debe hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis debe diseñarse una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

La política de seguridad es un “documento sencillo que define las directrices organizativas en materia de seguridad”. Ver Figura 5.

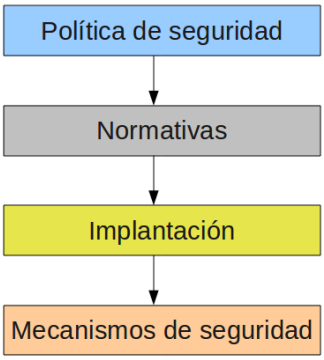

Figura 5 – Estructura de las políticas de seguridad

Los mecanismos de seguridad se dividen en tres grupos: preventivos, detectivos y correctivos.

Resumiendo, las políticas de seguridad deben contener claramente las prácticas que serán adoptadas por la organización. Y éstas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

2.1.5 Amenazas de TI

De forma general podemos agrupar las amenazas en: físicas y lógicas.

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por: personas, programas y desastres naturales.

El origen de las amenazas pueden ser: desastres naturales, agentes externos, y agentes internos. La intencionalidad de las amenazas son por: accidentes, errores, actuaciones malintencionadas.

2.1.6 Auditoría informática

Para garantizar un control de la seguridad de la información es necesario realizar periódicamente auditorías en informática, para comprobar la administración de todos los recursos de TI de la organización, con el fin de

emitir un informe y recomendaciones para el proceso de mejora continua. Las auditorías informáticas pueden ser internas y externas.

2.2 Glosario de términos

Seguridad de la información.- La seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información. (ISO 27000, 2014)

Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades. (Superintendencia de Bancos y Seguros, 2014)

Auditoría.- La auditoría informática es un proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. (ISO 27000, 2014)

Riesgo.- Riesgo es el efecto de la incertidumbre en los objetivos. (ISO 73, 2009)

SGSI o EGSI.- Un sistema de gestión de la seguridad de la información (SGSI) o Esquema Gubernamental de la seguridad de la información (EGSI), (en inglés: *information security management system*, ISMS) es, conjunto de elementos interrelacionados o que interactúan de una organización para

establecer las políticas, objetivos y procesos, para lograr esos objetivos. (ISO 27000, 2014)

Acuerdo 166.- Documento legal emitido por la SNAP, para el control de la seguridad de la información en las instituciones públicas del Estado Ecuatoriano.

Estándar o norma.- Es una especificación que reglamenta procesos y productos para garantizar la interoperabilidad.

Gobierno por resultados.- Es el conjunto de conceptos, metodologías y herramientas que permitirá orientar las acciones del gobierno y sus instituciones al cumplimiento de objetivos y resultados esperados en el marco de mejores prácticas de gestión. La aplicación de Gobierno Por Resultados permitirá una gestión eficiente de los planes estratégicos, planes operativos, riesgos, proyectos y procesos institucionales, en los distintos niveles organizacionales, a través de un seguimiento y control de los elementos, así como de los resultados obtenidos. (Secretaría Nacional de Administración Pública, 2011)

Alta gerencia.- La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada. (Superintendencia de Bancos y Seguros, 2014)

Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo. (Superintendencia de Bancos y Seguros, 2014)

Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo. (Superintendencia de Bancos y Seguros, 2014)

Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido. (Superintendencia de Bancos y Seguros, 2014)

Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio. (Superintendencia de Bancos y Seguros, 2014)

Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones. (Superintendencia de Bancos y Seguros, 2014)

Tecnología de la información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros. (Superintendencia de Bancos y Seguros, 2014)

Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos. (Superintendencia de Bancos y Seguros, 2014)

Incidente de tecnología de la información.- Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones

con probabilidad significativa de comprometer las operaciones del negocio; y, (Superintendencia de Bancos y Seguros, 2014)

Incidente de seguridad de la información.- Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Superintendencia de Bancos y Seguros, 2014)

2.3 Estado del Arte

2.3.1 Estado del Arte a nivel internacional

Existen varias normativas internacionales para implementar sistemas de control interno y de gestión de la seguridad de la información, los cuales son:

2.3.1.1 Normas internacionales de seguridad de la información:

La familia de normas ISO/IEC 27000, de las cuales las más importantes son:

- ISO/IEC 27000, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements,*
- ISO/IEC 27002, *Information technology -- Security techniques -- Code of practice for information security controls*
- ISO/IEC 27005, *Information technology -- Security techniques -- Information security risk management*

Certificación de ISO/IEC 27001

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado. (Campaña, 2010)

Antes de la publicación del estándar ISO 27001, las organizaciones interesadas en certificar su gestión de seguridad de la información lo hacían de conformidad con el estándar británico BS 7799-2. (COTECNA, 2015)

2.3.1.2 Códigos de buenas prácticas de seguridad de información

- COBIT 5.- COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los 5 principios de COBIT 5 y define los 7 catalizadores que componen el marco. (ISACA, 2015)

COSO.- *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) es una iniciativa conjunta de cinco organizaciones del sector privado y se dedica a proporcionar el liderazgo de pensamiento a través de la elaboración de marcos y orientación sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude. (COSO, 2015)

A más de 20 años de su emisión original, en mayo de 2013, COSO publicó la actualización al marco integrado de control interno ("COSO 2013") que sustituye al anterior COSO 1992. El nuevo marco es el resultado de una vasta aportación de distintos interesados del ambiente de negocios, firmas de auditoría, participantes en los mercados financieros y estudiosos del tema. (Price watherhouse Coopers, 2015)

COSO ERM Enterprise Risk Management – Integrated Framework [Administración del riesgo de la empresa – Estructura conceptual integrada] de COSO (la “estructura ERM”) no ha sido reemplazada por la estructura 2013. Si bien la estructura ERM y la estructura 2013 tienen la intención de tener diferentes centros de atención, las dos estructuras están diseñadas para complementarse una con la otra. COSO considera que si bien la estructura ERM incluye porciones del texto de la estructura 1992, la estructura ERM continúa siendo confiable para diseñar, implementar, dirigir, y valorar la administración del riesgo de la empresa. (Burns, 2013)

ITIL.- Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL®) se ha convertido en el estándar mundial de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL® es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización. (AXELOS, 2015)

2.3.1.3 Normas de Gobierno electrónico

ISO/IEC 38500, Corporate *Governance of Information Technology*

El **Gobierno de TI** es una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la empresa y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos. (NETWORK-SEC, 2015)

2.3.1.4 Normas de gestión del servicio

— ISO/IEC 20000, Information *technology -- Service management*

La ISO 20000 fue publicada en diciembre de 2005 y es la primera norma en el mundo específicamente dirigida a la gestión de los servicios de TI. La ISO 20000 fue desarrollada en respuesta a la necesidad de establecer procesos y procedimientos para minimizar los riesgos en los negocios provenientes de un colapso técnico del sistema de TI de las organizaciones. (OVERTI, 2015)

2.3.1.5 Normativa de Continuidad de Negocio

La continuidad del negocio (conocida en inglés como *Business Continuity*) describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre. La Planificación de la Continuidad del Negocio (BCP) trata de evitar la interrupción de los servicios de misión crítica y restablecer el pleno funcionamiento de la forma más rápida y fácil que sea posible. (PECB, 2015)

CAPÍTULO III

Metodología de Investigación

La metodología de investigación a usar será descriptiva y cualitativa, es decir, se va a diseñar una auditoría, con las fases de planificación, ejecución y entrega de resultados, con las técnicas de investigación de campo, entrevistas, encuestas, evidencia de los hallazgos. En este caso no se hará muestreo ya que se va a revisar el 100% de las normas o disposiciones de la Fase I, debido a que el universo es pequeño y se debe revisar todos los puntos de la Fase I.

Ninguna etapa de esta metodología debe estar en desacuerdo con los métodos de investigación científica.

La metodología será deductiva, es decir, parte de lo general para realizar inferencias específicas.

Se va a partir del estudio del estado del arte de la Seguridad de la Información, a partir de las normas y Buenas Prácticas, aceptadas a nivel internacional.

Se va a realizar una evaluación técnica del cumplimiento de la Fase I del Acuerdo 166 en el CEAACES, para verificar el porcentaje de cumplimiento y si se lo hizo en los plazos establecidos.

Debido a esta metodología la investigación será descriptiva y evaluativa.

Se va a utilizar las siguientes técnicas de investigación:

Documental: Recopilación de información para enunciar las teorías que sustentan el estudio de los fenómenos y procesos, se va a investigar las

normativas y códigos de buenas prácticas generalmente aceptadas a nivel internacional para la Seguridad de la Información.

De campo: Permite la observación en contacto directo con el sujeto de estudio, y el acopio de testimonios para confrontar la teoría con la práctica. Se va a hacer una inspección en las instalaciones del CEAACES y entrevistar a los directores y personal técnico y administrativo de la institución.

Las variables a ser consideradas en esta investigación serán cualitativas en el nivel de cumplimiento de las disposiciones y fechas.

En esta investigación no se hará ninguna forma de muestreo ya que se va a investigar el total de las disposiciones, debido a dos razones, porque se debe revisar todas y cada una de las normas de la Fase I del Acuerdo 166, y que en la planificación debe contener todos los puntos de la Fase I.

Las técnicas de investigación serán las siguientes:

- Entrevista
- Encuesta
- Revisión de los documentos de la institución

3.1. Enfoque metodológico de la auditoría

El enfoque metodológico propuesto integra el conocimiento aportado por las organizaciones que lideran el desarrollo de los estándares y mejores prácticas en el ámbito de las tecnologías de la información reconocidas a nivel internacional, entregando un marco referencial para realizar auditorías a las tecnologías de información centradas en los procesos del negocio, los sistemas de información que los soportan y sus actividades de control. (Ibsen. S., & Yañez de la Melena, C., 2011)

3.2. Etapas de la Metodología de Auditoría

Esta metodología constituye una herramienta basada en el estándar COBIT y la norma técnica ISO/IEC 27002 a los programas de auditorías a las tecnologías de información y comunicaciones.

A continuación, se presentan las etapas que componen la metodología:

FASE I. Planificación de la auditoría

1. Plan de auditoría preliminar
2. Comprensión de la organización, procesos de negocio y sistemas
3. Definición del programa y alcance de la auditoría

FASE II. Ejecución de la auditoría

4. Evaluación del control interno
5. Diseño de las pruebas de auditoría
6. Ejecución de las pruebas de auditoría
7. Evaluación del resultado de las pruebas de auditoría

FASE III. Comunicación de los resultados

8. Elaboración del informe con los resultados de la auditoría
9. Seguimiento a las observaciones de la auditoría

3.2.1. Fase I. Planificación de la auditoría

La primera fase de la auditoría consiste en realizar un levantamiento de la situación actual y su manejo con respecto al Acuerdo 166, se establece el equipo de auditores conformados por los ingenieros César Cabrera y Juan

Morejón, se indican los tiempos necesarios para la realización de la verificación.

La siguiente etapa que es la asimilación de los procesos internos que se manejan y el levantamiento de la información necesaria para la elaboración del estado actual y características de la Institución así como de todos sus recursos técnicos y tecnológicos.

La auditoría va a estar enfocada a la evaluación técnica de la implementación de la Fase I establecida en la normativa técnica del Ecuador, NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Se estableció el levantamiento de la información según el cronograma presentado, para la revisión de los 11 componentes de esta norma técnica.

Tabla 1 – Cronograma de la auditoría

	Semana 1					Semana 2					Semana 3					Semana 4					Semana 5			
Actividad	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4
Plan de auditoría	x																							
Definición de los objetivos y alcance de la auditoría	x																							
Giro del negocio de la organización , procesos y sistemas		x	x	x																				
Evaluación del Control Interno					x	x	x	x	x	x	x	x	x	x	x	x	x	x						
Definición y diseño de pruebas																			x	x	x			
Ejecución de pruebas																						x		
Análisis de resultados																						x		
Elaboración de informe																							x	x

3.2.2. Fase II. Ejecución de la auditoría

Los 11 componentes fueron realizados acorde al cronograma, se empleó el mes de enero y parte de febrero para la revisión de los siguientes componentes:

- Política de seguridad de la información (2)
- Organización de la seguridad de la información (6)
- Gestión de los activos (7)
- Seguridad de los recursos humanos (3)
- Seguridad física y del entorno (12)
- Gestión de comunicaciones y operaciones (28)
- Control de acceso (36)
- Adquisición, desarrollo y mantenimiento de sistemas de información (2)
- Gestión de los incidentes de la seguridad de la información (2)
- Gestión de la continuidad del negocio (0)
- Cumplimiento (0)

La siguiente etapa consiste en definir y diseñar las pruebas de auditoría tanto las de cumplimiento para los controles claves de los procesos de negocio y sistemas agrupados por técnicas de verificación como las sustantivas para datos clave de los procesos y sistemas.

Para finalizar esta fase se evalúan los resultados obtenidos en las pruebas de auditoría, realizando un análisis de las observaciones de auditoría y puntos mejorables para los controles y datos deficientes, identificando las causas, el impacto y las implicaciones de las observaciones para la organización y verificar los estándares y mejores prácticas que no se cumplen.

Como fin de esta fase se elaboran las conclusiones de auditoría para los resultados no satisfactorios.

3.2.3. Fase III. Comunicación de los resultados

Esta es la última fase de la auditoría, en ella se resumen los resultados más significativos obtenidos en las etapas anteriores.

Estos son los insumos para elaborar el informe de auditoría con el cual se comunicará a la alta dirección y a los demás interesados, las observaciones y conclusiones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

La etapa de seguimiento a las observaciones de auditoría ya no será realizada ya que se encuentra fuera del alcance del proyecto, y será la entidad receptora del proyecto la encargada de su ejecución.

Para lo cual se elabora el resumen de observaciones que servirá de base para desarrollar y aprobar informe preliminar; luego se analizará respuesta del servicio al informe preliminar para diseñar las conclusiones generales y específicas de la auditoría. Para finalizar con la elaboración y aprobación y emisión del informe final de auditoría.

Organizar y cerrar expediente y archivo con hojas de trabajo.

Tabla 2 – Etapas de la metodología de auditoría. Fase I

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	DESCRIPCIÓN		
1	**Plan de auditoría preliminar**	• Elaborar un plan de auditoría con objetivos generales. • Conformar el grupo de trabajo que realizará la auditoría. • Estimar tiempo necesario para realizar la auditoría.	• Definición del perfil del personal requerido y asignación de auditores. • Lista con horas estimadas por etapa para realizar la auditoría.
2	**Comprensión de la organización, procesos de negocio y sistemas**	• Recolectar flujograma de los procesos de negocio.	• Documento con definición de los procesos de negocio y diagramas descriptivos.
3	**Definición del programa y alcance de la auditoría**	• Elaborar el programa de auditoría detallado. • Confeccionar Diagrama Gantt del programa de auditoría.	• Programa de auditoría detallado. • Diagrama Gantt del programa de auditoría.

Tabla 3 – Etapas de la metodología de auditoría. Fase II

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	DESCRIPCIÓN		
4	**Evaluación del sistema de control interno**	• Identificar y documentar los controles existentes en los procesos de negocio y sistemas de información.	• Lista de controles que deben ser cumplidos por la institución.
5	**Definición y diseño de las pruebas de auditoría**	• Verificar el cumplimiento de los controles obligatorios de los controles prioritarios.	• Matriz con el listado de controles prioritarios.
6	**Ejecución de las pruebas de auditoría**	• Ejecutar pruebas de cumplimiento de los controles prioritarios recolectados utilizando técnicas de verificación manuales o asistidas por computador.	• Lista de controles verificados por el auditor.
7	**Evaluación de los resultados obtenidos en las pruebas de auditoría**	• Evaluar los resultados de las pruebas efectuadas. • Desarrollar el análisis de las observaciones de auditoría y puntos mejorables para los controles y datos deficientes. • Identificar las causas, el impacto y las implicaciones de las observaciones para la organización y verificar los estándares y mejores prácticas que no se cumplen. • Diseñar las conclusiones de auditoría para los resultados no satisfactorios.	• Listado con análisis de observaciones de auditoría para pruebas de cumplimiento y sustantivas. • Conclusiones de los resultados obtenidos.

Tabla 4 – Etapas de la metodología de auditoría. Fase III

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
Nº	DESCRIPCIÓN		
8	**Elaboración del informe con los resultados de la auditoría**	• Elaborar resume de observaciones. • Desarrollar y aprobar informe preliminar. • Emitir informe preliminar. • Analizar respuesta del servicio al informe preliminar. • Diseñar conclusiones generales y específicas de la auditoría. • Elaborar y aprobar informe final de auditoría. • Emitir informe final de auditoría. • Organizar y cerrar expediente y archivo con hojas de trabajo.	• Resumen de observaciones obtenidas. • Informe preliminar de auditoría. • Documento con el análisis de las respuestas emitidas por el servicio auditado al informe preliminar. • Informe final de auditoría. • Expediente de auditoría con observaciones organizadas y referenciadas adecuadamente.
9	**Seguimiento a las observaciones de auditoría**	• Planificar seguimiento al cumplimiento de las observaciones de auditoría. • Efectuar seguimiento en fechas programadas. • Analizar y evaluar resultados del seguimiento. • Elaborar y aprobar informe de seguimiento. • Emitir informe de seguimiento.	• Programa de seguimiento. • Listado con el resultado del cumplimiento de las observaciones. • Informe de seguimiento.

3.3 Proceso de auditoría

3.3.1 Plan de auditoria preliminar

Se establece como auditores externo para la realización de esta auditoría a los maestrantes que están realizando esta tesis.

El tiempo estimado para la realización de la misma está establecido según la siguiente definición:

Tabla 5 – Etapas de la metodología de auditoría. Fase II

Actividad	Responsable	Tiempo
Control componentes 1 y 2	Juan Morejón	16 h
Control componente 3	César Cabrera	8 h
Control componente 4	Juan Morejón	8 h
Control componente 5	César Cabrera	8 h
Control componente 6	Juan Morejón César Cabrera	8 h
Control componente 7	Juan Morejón César Cabrera	52 h
Control componente 8	Juan Morejón	6 h
Control componente 9	César Cabrera	6 h

3.3.2 Compresión de la organización, procesos de negocio y sistemas

Se estudia, observa y familiariza con el ambiente institucional, se realizan reuniones con las principales personas que están a cargo del manejo del SGSI solicitándoles información inicial de como se ha venido cumpliendo con el Acuerdo 166.

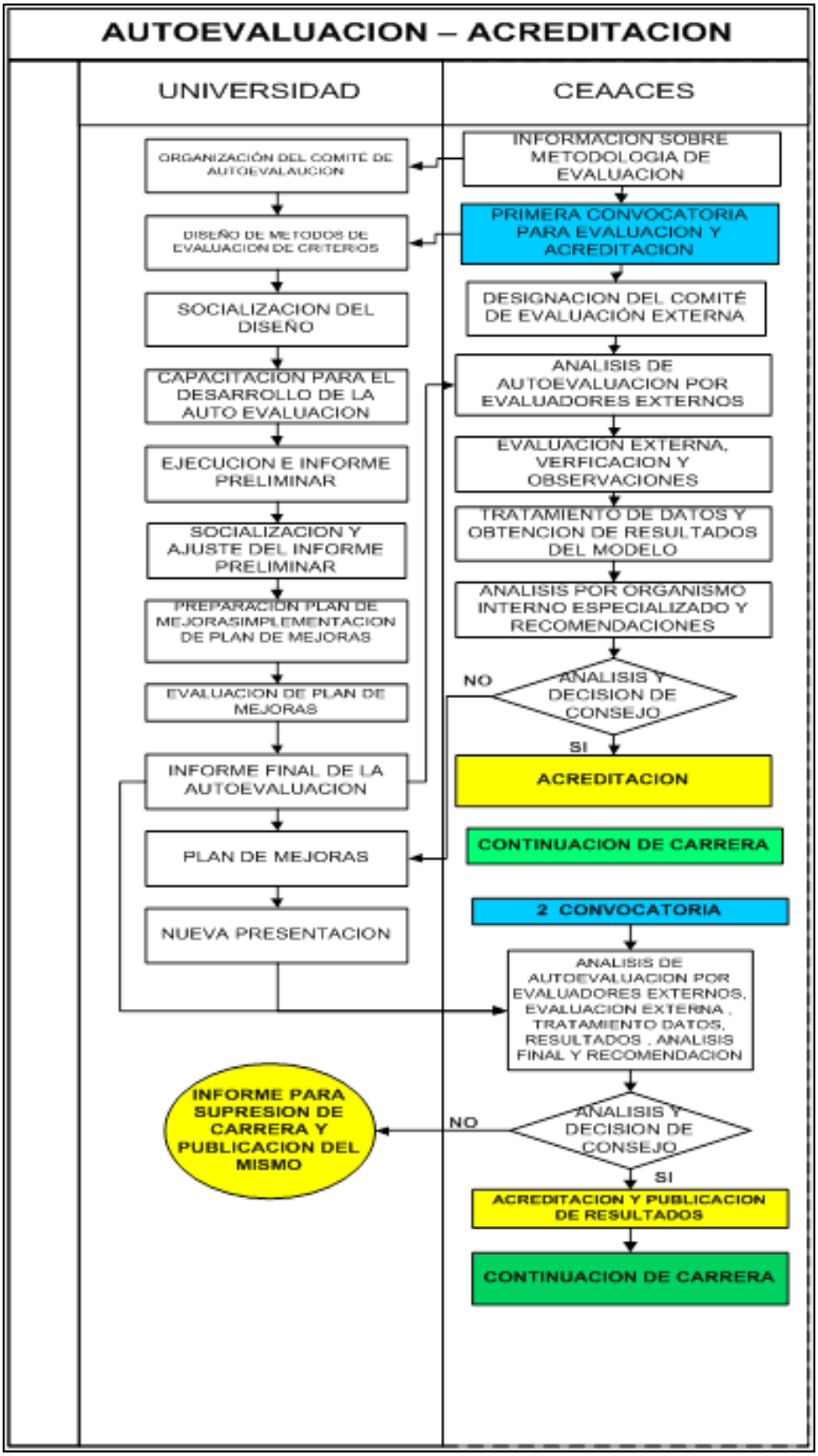

Figura 6 – Flujograma de los procesos acreditación de Instituciones de Educación Superior

3.3.3 Definición del programa y alcance de la auditoría

Son 11 componentes y 98 controles que comprenden la fase I del EGSI, lo que debe ser aplicado por la Institución de manera obligatoria con el 100% de cumplimiento.

Tabla 6 – Tiempo por cada etapa de la auditoría

#	Etapa	Tiempo
1	Plan de auditoria	4 h
2	Definición del objetivos y alcance de la auditoría	4 h
3	Giro del negocio de la organización, procesos y sistemas	24 h
4	Evaluación del Control Interno	112 h
5	Definición y diseño de pruebas	24 h
6	Ejecución de pruebas	4 h
7	Análisis de resultados	4 h
8	Elaboración de informe	16 h

	Nombre de tarea	Duración	Comienzo	Fin	Pred
1	Plan de auditoria	4 horas	lun 05/01/15	lun 05/01/15	
2	Definición del objetivos y a	4 horas	lun 05/01/15	lun 05/01/15	1
3	Giro del negocio de la orga	3 días	mar 06/01/15	jue 08/01/15	2
4	Evaluación del Control Inte	14 días	vie 09/01/15	mié 28/01/15	3
5	Definición y diseño de pru	3 días	jue 29/01/15	lun 02/02/15	4
6	Ejecución de pruebas	4 horas	mar 03/02/15	mar 03/02/15	5
7	Análisis de resultados	4 horas	mar 03/02/15	mar 03/02/15	6
8	Elaboración de informe	2 días	mié 04/02/15	jue 05/02/15	7

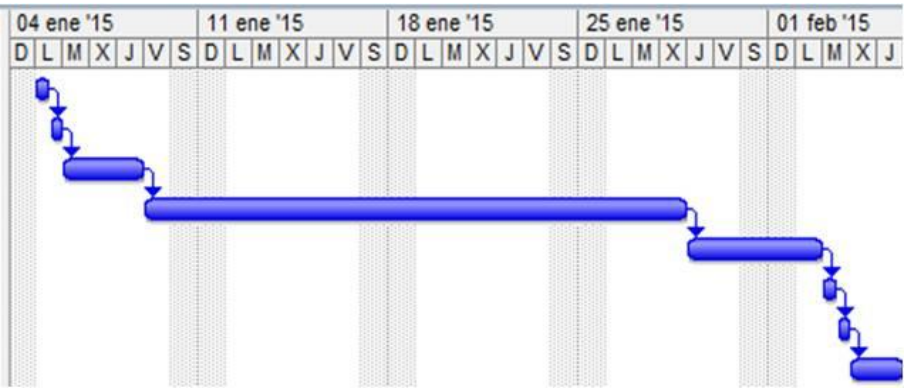

Figura 7 – Mapa de Gantt de la planificación de la auditoría

3.3.4 Evaluación del Sistema de Control interno

Los controles para esta auditoría son los marcados como prioritarios en el Acuerdo 166, y están marcados con un asterisco. Para la totalidad de los controles del Acuerdo 166, ver el Anexo A.

3.3.5 Definición y diseño de las pruebas de auditoría

Realizar una revisión sistemática de cada uno de los 98 controles marcados como prioritarios, evidenciar su cumplimiento en una matriz con la observación de su cumplimiento.

El diseño de los controles prioritarios consiste en una tabla de Excel, que tiene 3 columnas:

- Cumplimiento: Aquí se debe marcar la opción Si/No.
- Evidencia: El documento que respalda la verificación del control.
- Observación: Si ha habido información relevante en la verificación de cada control.

1. Política de seguridad de la información (2)

1.1. Documento de la Política de la Seguridad de la Información

Control	Cumplimiento	Evidencia	Observación
a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad	Si	Memorando Nro. CEAACES-P-2014-0078-M	Documento EGSI_CEAACES_1.1.1_P_01_29-09-2014.pdf
b) Se difundirá la siguiente política de seguridad de la información como referencia (*):	Si	Acta de Reunión No. 006 CSI de 22708/2014 Informe de capacitación en Seguridad de la Información. RESOLUCIÓN No. 081-P-CEAACES-2014	Documento EGSI_CEAACES_1.1.2_P_01_29-09-2014.pdf

Figura 8 – Diseño de la verificación del control

3.3.6 Ejecución de las pruebas de auditoría

La revisión de los 98 controles prioritarios, se lo hace evidenciando su cumplimiento en una matriz de control, el archivo utilizado durante la auditoría se detallan en el Anexo B, Cumplimiento de Controles Prioritarios.

3.3.7 Evaluación de los resultados obtenidos en las pruebas de auditoría

Al ser mandatorio enviar los avances de la auditoria de la implementación de la Fase I, es necesario llenar un informe de cumplimiento de hitos diseñado por la SNAP, donde tiene varios campos que especifican el nombre de la institución, la codificación y el nombre del control, y las tareas realizadas. Ver Figura 9.

En el Anexo C se muestran los informes de cumplimiento de hitos.

SISTEMA DE GOBIERNO POR RESULTADOS (GPR)			
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):	*CONSEJO DE EVALUACION ACREDITACION Y ASEGURAMIENTO DE LA CALIDAD DE LA EDUCACION SUPERIOR*		
DENOMINACIÓN DEL HITO:	*RETIRAR INFORMACIÓN IMPRESA UNA VEZ QUE SEA IMPRESA*		
NÚMERO DE HITO:	7.8.4	ES UN HITO PRIORITARIO?	*SI*
No.	RESUMEN ACTIVIDADES REALIZADAS	VERIFICABLE INTERNO	
1	Aplicación de procedimiento PL-TIC-TI-001 para tratamiento de información impresa	Procedimiento PL-TIC-TI-001	

Figura 9 – Ejemplo de hitos de cumplimiento para ser enviados a la SNAP

3.3.8 Elaboración del informe con los resultados de la auditoría

En esta parte se exponen los resultados de las actividades previas las cuales indican a la alta gerencia las falencias en las cuales esta incursa la Institución, esto ayudará a tomar las decisiones adecuadas para el manejo de las no conformidades existentes para el cumplimiento del Acuerdo 166.

3.4 Mapa de riesgos

3.4.1 Metodología de mapeo de riesgos

El análisis del riesgo para que sea eficiente se lo debe hacer con dos variables los cuales son el impacto y la vulnerabilidad, al combinar estas dos variables, tenemos el riesgo de una forma cuantitativa. Las respuestas obtenidas son promediadas, y dependiendo del resultado se activan unas celdas de la siguiente manera:

Valoración	Color
Bajo	
Medio	
Alto	

Para realizar este análisis se consultó a tres colaboradores de la organización, los cuales daban una valoración de 1 a 5, siendo 1 muy baja/improbable hasta el 5 muy alta/probable.

Para tener una opinión global de la organización, estas personas deben venir de diferentes departamentos, siendo apenas uno el que se dedica a tecnología. Los otros son un asesor de la Presidencia y el Director del Departamento Administrativo. Ver Figura 10.

ceaaces
CONSEJO DE EVALUACIÓN, ACREDITACIÓN Y ASEGURAMIENTO DE LA CALIDAD DE LA EDUCACIÓN SUPERIOR

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Diligencie solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos.

	PROCESO	LIDER PROCESO	TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Ing. Alvaro Buestán (Analista TICS)	Calificación Ing. Iván Cuenca (Asesor)	Calificación Eco. Holger Agila (Jefe Administrativo)
R1	POLÍTICA SI	Alta Gerencia	R1	No disponer de un documento de la Política de la Seguridad		Bajo	2,0	1,3	VOTO IMPACTO	1,0	2,0	1,0
									VOTO VULNERABILIDAD	3,0	2,0	1,0
R2	ORGANIZACIÓN SI	CSI	R2	No cumplir los acuerdos de Confidencialidad		Bajo	1,7	1,3	VOTO IMPACTO	1,0	1,0	2,0
									VOTO VULNERABILIDAD	1,0	2,0	2,0
R3	GESTIÓN ACTIVOS	Jefe TICS	R3	No tener actualizado el inventario y ubicación de activos de soporte		Bajo	1,7	1,7	VOTO IMPACTO	1,0	2,0	2,0
									VOTO VULNERABILIDAD	2,0	2,0	1,0
R4	RECURSOS HUMANOS	Jefe TICS	R4	Tener colaboradores que sean una amenaza para la institución		Bajo	1,3	1,3	VOTO IMPACTO	2,0	1,0	1,0
									VOTO VULNERABILIDAD	1,0	2,0	1,0
R5	SEGURIDAD FÍSICA Y DEL ENTORNO	Jefe TICS	R5	Accesos no autorizados a oficinas, recintos e instalaciones		Bajo	1,3	2,0	VOTO IMPACTO	1,0	2,0	3,0
									VOTO VULNERABILIDAD	1,0	2,0	1,0
R6	SEGURIDAD FÍSICA Y DEL ENTORNO	Jefe TICS	R6	Destrucción de las instalaciones debido a amenazas externas y		Medio	2,7	3,0	VOTO IMPACTO	3,0	3,0	3,0
									VOTO VULNERABILIDAD	2,0	3,0	3,0
R7	SEGURIDAD FÍSICA Y DEL ENTORNO	Jefe TICS	R7	Caída del servicio de energía eléctrica		Medio	2,7	2,0	VOTO IMPACTO	1,0	2,0	3,0
									VOTO VULNERABILIDAD	2,0	3,0	3,0
R8	SEGURIDAD FÍSICA Y DEL ENTORNO	Jefe TICS	R8	Caídas del servicio de internet, intranet y comunicaciones		Bajo	2,0	1,7	VOTO IMPACTO	2,0	1,0	2,0
									VOTO VULNERABILIDAD	2,0	1,0	3,0
R9	COMUNICACIONES Y OPERACIONES	Jefe TICS	R9	Caída del servicio por no gestionar la capacidad y el		Medio	1,7	3,7	VOTO IMPACTO	4,0	3,0	4,0
									VOTO VULNERABILIDAD	2,0	1,0	2,0
R1	COMUNICACIONES Y OPERACIONES	Jefe TICS	R10	Penetración de código malicioso en el sistema		Medio	2,3	3,3	VOTO IMPACTO	2,0	3,0	5,0
									VOTO VULNERABILIDAD	2,0	2,0	3,0
R1	COMUNICACIONES Y OPERACIONES	Jefe TICS	R11	Pérdida de información crítica		Alto	4,3	4,3	VOTO IMPACTO	5,0	5,0	3,0
									VOTO VULNERABILIDAD	4,0	5,0	4,0
R1	CONTROL DE ACCESO	Jefe TICS	R12	Fuga de información sensible		Medio	4,0	3,3	VOTO IMPACTO	4,0	3,0	3,0
									VOTO VULNERABILIDAD	3,0	5,0	4,0
R1	CONTROL DE ACCESO	Jefe TICS	R13	No realizar autenticación de usuarios para		Bajo	1,3	2,3	VOTO IMPACTO	2,0	2,0	3,0
									VOTO VULNERABILIDAD	2,0	1,0	1,0
R1	CONTROL DE ACCESO	Jefe TICS	R14	Intrusión por no realizar la protección de los puertos de		Medio	2,0	3,0	VOTO IMPACTO	2,0	3,0	4,0
									VOTO VULNERABILIDAD	2,0	2,0	2,0
R1	CONTROL DE ACCESO	Jefe TICS	R15	Acceso no autorizados por no realizar la separación de		Bajo	1,7	1,3	VOTO IMPACTO	1,0	2,0	1,0
									VOTO VULNERABILIDAD	2,0	2,0	1,0
R1	CONTROL DE ACCESO	Jefe TICS	R16	No realizar la identificación y autenticación de		Bajo	1,3	1,7	VOTO IMPACTO	2,0	2,0	1,0
									VOTO VULNERABILIDAD	1,0	1,0	2,0
R1	CONTROL DE ACCESO	Jefe TICS	R17	Accesos no autorizados por medio de computación y		Medio	1,3	3,3	VOTO IMPACTO	3,0	5,0	2,0
									VOTO VULNERABILIDAD	1,0	1,0	2,0
R1	ADQUISICIÓN, DESARROLLO, Y MANTENIMIENTO	Jefe TICS	R18	Fallas de requisitos de seguridad en el lanzamiento a		Bajo	1,7	2,0	VOTO IMPACTO	2,0	3,0	1,0
									VOTO VULNERABILIDAD	1,0	2,0	2,0
R1	GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA	Jefe TICS	R19	No realizar reportes sobre los eventos de seguridad de la		Bajo	2,3	1,3	VOTO IMPACTO	2,0	1,0	1,0
									VOTO VULNERABILIDAD	3,0	2,0	2,0

Figura 10 – Valoración de impacto y vulnerabilidad de los riesgos

Antes de esta valoración se enlistó los principales riesgos de no efectuar los controles descritos en el Acuerdo 166. En total se obtuvo 37 riesgos que deben ser cuantificados por personal de la organización.

Al realizar un mapeo de riesgos de forma gráfica, conocido como mapa de riesgos, tiene la ventaja importante que es más fácil descubrir los riesgos de alto impacto y vulnerabilidad, que si se lo presentara en forma numérica. Es una técnica muy utilizada en auditoría informática basada en riesgos.

El mapa de riesgos se lo realiza dibujando una tabla, con la escala de vulnerabilidad en el eje horizontal, y la escala de impacto en el eje vertical. Se utiliza el color verde para niveles bajos, el color amarillo para niveles medios y el color rojo para niveles altos. Al ubicarse los riesgos según su valoración es fácil para la Dirección ver claramente donde se deben enfocar los esfuerzos de mejora.

3.4.2 Valoración del riesgo mediante su impacto y probabilidad.

Al ser siempre los recursos escasos, la organización debe enfocarse en asignar los recursos a los controles que minimizan los riesgos más críticos. Del análisis realizado se han escogido los cinco riesgos más peligrosos para la entidad: Ver Figura 11.

- Destrucción de instalaciones debido a amenazas externas y ambientales

- Robo de información por no monitorear y revisar los servicios prestados por terceros.

- Penetración de código malicioso en el sistema

- Pérdida de información por no hacer respaldos de la información

- Fuga de información sensible por no realizar gestión de contraseñas para usuarios

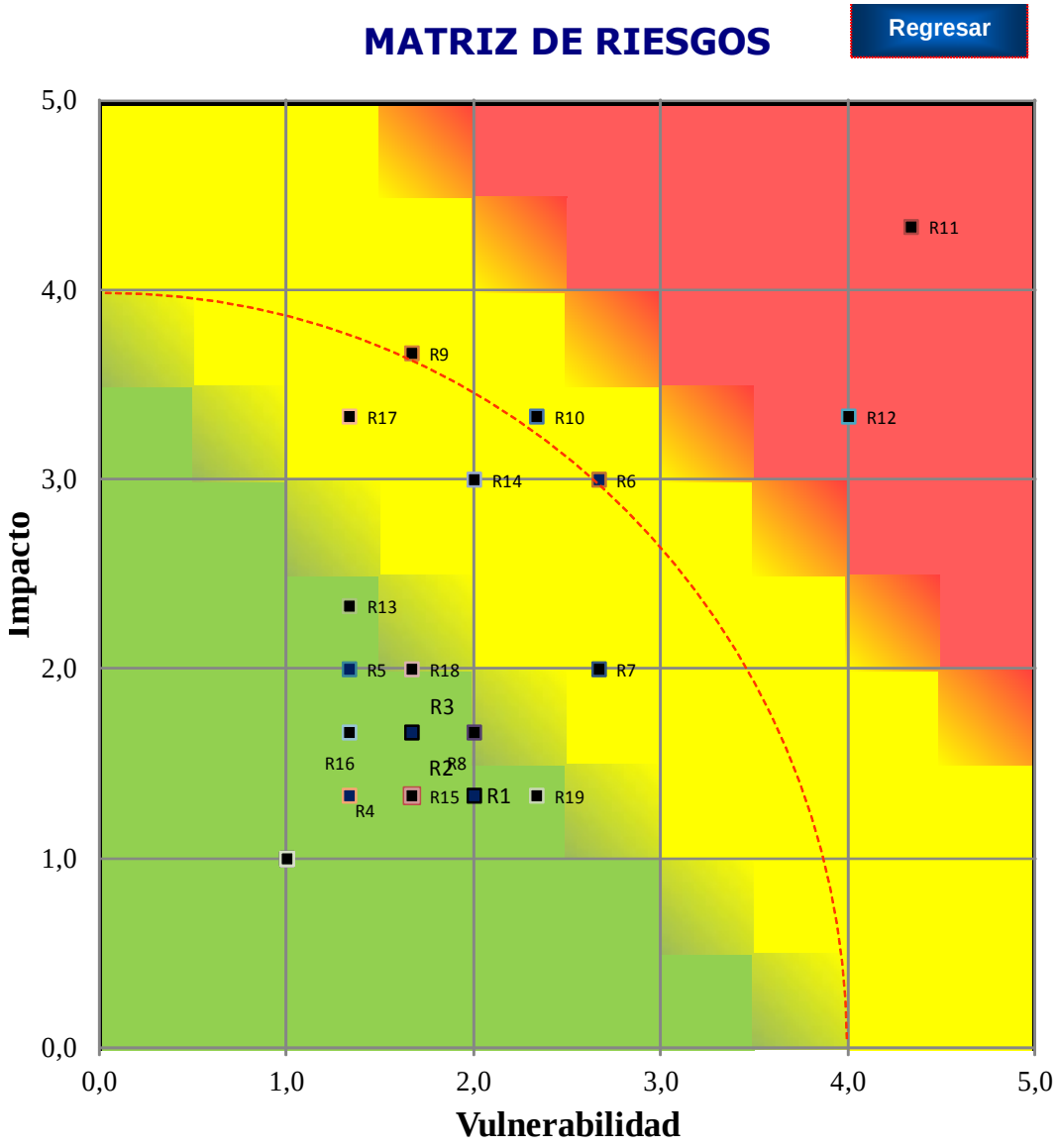

Figura 11 – Mapa de riesgos de forma gráfica

Estos riesgos si no se monitorean con controles eficientes y constantes, pueden producir daños irreversibles económicos y de imagen, con el agravante de que el CEAACES al manejar información sensible de las Instituciones de Educación Superior y ser parte de la Administración Central, el Gobierno resulte afectado en su imagen, ya que la fuga o perdida de la información podría ser utilizada con fines políticos.

3.5 Seguimiento a las observaciones de auditoria

El actual estudio no contempla el seguimiento de las no conformidades ni de las recomendaciones que se establecen en el presente informe.

3.6 Conclusiones

- Se puede observar en la tabla del cumplimiento de los controles de la Fase I del Acuerdo 166, que todos fueron cumplidos, adjuntado la evidencia en cada caso. Sin embargo, ninguno de ellos fue cumplido en el plazo previsto de que obligaba tenerlos listos 6 meses después de la oficialización del Acuerdo 166. La Fase I debió estar cumplida en su totalidad el mes de marzo de 2014, ya que el Acuerdo 166 se emitió en septiembre de 2013, ya que los últimos informes de cumplimiento fueron entregados en diciembre de 2014.

- En el Dominio 4 Seguridad de los Recursos Humanos, numeral 4.1 literal a) indica que al momento de la contratación del personal la Unidad de Talento Humano debe pedir el Certificado de Antecedentes Penales, este control se ha vuelto polémico en el Ecuador ya que se establece como ilegal por parte del Ministerio de Interior el solicitarlo tanto en el sector público como el privado.

- Se detectó que existe un alto nivel de vulnerabilidad en caso de que por alguna razón se pierdan algo de la información considerada como crítica, previo a alguno de los procesos de evaluación que la Institución realizada.

- Se estableció que podría existir fuga parcial de la información sensible que las Instituciones de Educación Superior confían para los procesos de Evaluación y Acreditación.

- Se detectó que existe una alta rotación de personal que se encuentra bajo la modalidad de contrato, en los cuales se invirtió recursos para prepararlos y estos no fueron revertidos en su totalidad dentro de la Institución, los nuevos ingresos consumen recursos para poder ser preparados y acoplarse a las funciones que se les encarga.

3.7 Recomendaciones

- Los controles que tienen como base documentos como: políticas, procedimientos, instructivos, etc., deben ser socializados al interior de la Institución, ya que los colaboradores no conocen y no cumplen con las obligaciones que poseen estos documentos, ya que existen gran rotación de funcionarios (entre el 45 y 60%) en la Institución esto debería llevarse en campañas frecuentes para evitar incumplimientos involuntarios por desconocimiento por parte de algún funcionario.

- Se deberá establecer plazos más cortos dentro del Plan de Recuperación de Desastres y Continuidad del Negocio, ya que el tiempo es importante estando previo a un proceso de Evaluación, debido a que se corren tiempos para cada una de las etapas.

- Se deberá seccionar y limitar la cantidad y nivel de acceso a la información que se tiene por cada uno de los técnicos que reciben y verifican la información que podría catalogarse como sensible de las Instituciones de Educación Superior. De esta forma se podrá minimizar la posibilidad de pérdida total de información sensible o crítica, ya que CEAACES es una Institución referente nacional y la única que por mandato está obligada a hacer las evaluaciones, acreditaciones y el aseguramiento de la calidad que las mismas prestan a la ciudadanía, la Institución es estratégica para el Gobierno Nacional y su política de mejoramiento de la Educación Superior.

CAPÍTULO IV

4.1 Conclusiones

Al realizar esta auditoría se ha podido observar que no se logró el cumplimiento de la Fase I en la fecha propuesta, lo que da a entender que el tiempo dado por la SNAP fue insuficiente para las instituciones públicas, en este caso el CEAACES, o que la institución no comprometió los recursos suficientes para cumplir el plazo propuesto para la implementación de la Fase I.

Al ser el CEAACES una institución del Estado, el cumplimiento se mide a través de GPR, administrada por la SNAP, lo que centraliza el manejo de la Gestión de la Seguridad de la Información de todo el Estado en una sola institución.

La metodología propuesta por Carlos Yañez de la Melena y Sigfrid Enrique Ibsen Muñoz, ganadora del Primer Premio por el OLACEFS ha demostrado ser muy eficiente y de fácil aplicación, por lo que se recomienda fuertemente para futuras auditorias informáticas, ya que describe muy bien los pasos a seguir y los documentos entregables en cada etapa de la auditoría.

En el país existen muy pocas empresas certificadas en la norma ISO 27001, lo que denota que debe haber un gran trabajo de las organizaciones privadas y públicas en lo referente Gestión de Seguridad de la Información, sobretodo en el tema de cumplimiento de normativas y buenas prácticas internacionales, ya que esto implica un cambio de pensamiento, cultural, buenas prácticas aplicadas a la vida diaria.

La implementación de un SGSI, puede ser realizado por una variedad de software especializado en el tema, entre los más conocidos son: ePULPO,

AGGIL, Gesconsultor, SECURIA SGSI, entre otros. Estos sistemas ofrecen automatizar todo el proceso de implantación, puesta en funcionamiento, control y mejora de un SGSI.

Hay que anotar que las normas ISO no son las únicas en cuanto a controles de un SGSI, sin embargo al ser ISO la Organización Internacional de Normalización, está más aceptada a nivel mundial. Existe mucha información sobre como alinear los controles de ISO 27000, COBIT e ITIL, que son los estándares más aplicados en la actualidad.

En el Dominio 4 Seguridad de los Recursos Humanos, numeral 4.1 literal a) indica que al momento de la contratación del personal la Unidad de Talento Humano debe pedir el Certificado de Antecedentes Penales, este control se ha vuelto polémico en el Ecuador ya que se establece como ilegal por parte del Ministerio de Interior el solicitarlo tanto en el sector público como el privado.

4.2 Recomendaciones

El Acuerdo 166 se basa en la norma técnica ecuatoriana NTE INEN ISO/IEC 27002:2009, *Tecnología de la información. Técnicas de la seguridad. Código de práctica para la Gestión de la Seguridad de la Información*, que a su vez es una adopción idéntica de la norma internacional ISO 27002:2005. Esta norma internacional fue revisada por lo cual la versión actual es del año 2013, ISO 27002:2013, *Information technology -- Security Techniques -- Code of Practice for Information Security Controls*, por lo que el Acuerdo 166 debería actualizarse ya que existen nuevos controles y dominios en la normativa de Seguridad de la Información.

Diseñar un control para evaluar periódicamente si los colaboradores de la institución están aplicando los controles establecidos en las Políticas de Seguridad como son los procedimientos e instructivos de la Seguridad de la Información para comprobar que los documentos no sean ignorados por los funcionarios.

Al ingreso de nuevo funcionario, debe darse una jornada de inducción la misma que a más de la Dirección de Talento Humano debe contar con el apoyo de la Unidad de Seguridad de la Información y de la Unidad de Tecnologías de la Información y Comunicación, en la que a más de las funciones propias del puesto y el conocimiento general de la Institución se sume el tema de Seguridad Informática.

Sugerir al Departamento de Talento Humano, se coordine capacitaciones periódicas para el personal acerca de aplicar las mejores prácticas en cuanto a la Gestión de la Seguridad de la Información, ya que en muchas empresas la fuga de información ocurre por cuestiones no técnicas sino más bien por ataques de ingeniería social.

En las próximas auditorias informáticas del Acuerdo 166, se debería considerar el realizar un análisis de madurez a la aplicación de los controles y no quedarse simplemente con la variable si cumple o no cumple el control, con un checklist.

Realizar un registro completo de todos los incidentes relacionados al SGSI, para tener mejor documentado los posibles ataques recibidos y la forma en que se solucionaron y buscar maneras para evitarlos.

Bibliografía

AXELOS. (12 de marzo de 2015). *Itil. Axelos*. Obtenido de Axelos: https://www.axelos.com

Burns, J. &. (2013). *COSO mejora su Control Interno - Estructura conceptual integrada.* Heads Up, 20, 16.

Campaña, O. (8 de abril de 2010). *Universidad Politénica Salesiana*. Obtenido de Universidad Politénica Salesiana: http://dspace.ups.edu.ec/bitstream/123465789/4468/1/UPS-ST000352.pdf

CEAACES. (23 de Enero de 2014). *Que hacemos: Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior*. Obtenido de Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior: http://ceaaces.gob.ec/sitio/que-hacemos/

CES. (4 de febrero de 2015). *Misión, Visión, Objetivos: Consejo de Educación Superior*. Obtenido de Consejo de Educación Superior: http://www.ces.gob.ec/institucion/mision-vision-y-objetivos

COSO. (11 de marzo de 2015). *Home: Committee of Sponsoring Organizations of the Treadway Commission*. Obtenido de Committee of Sponsoring Organizations of the Treadway Commission: http:www.coso.org

COTECNA. (11 de marzo de 2015). *Certificación ISO 27001: COTECNA*. Obtenido de COTECNA: http://www.cotecna.com.ec/~/media/Countries/Ecuador/Documents/Brochure-iso-27001-cotecna-ecuador-FINAL.ashx?la=es-ES

Ibsen. S., & Yañez de la Melena, C. (19 de enero de 2011). *Enfoque metodológico de la Auditoría a las Tecnologías de la Información*. Obtenido de Olacefs: http://www.olacefs.com/wp-content/plugins/google-document-embedder/load.php?d=http%3A%2F%2Fwww.olacefs.com%2Fwp-content%2Fuploads%2F2014%2F08%2F1erlugar.pdf

ISACA. (17 de febrero de 2015). *Spanish: Information System Audit and Control Association*. Obtenido de Information System Audit and Control Association: http://isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISO 27000. (2014). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario Términos y definiciones.* Ginebra: Organización Internacional de Normalización.

ISO 73. (2009). *Organización Internacional de Normalización Guide 73.* Ginebra: ISO.

Mifsud, E. (7 de abril de 2015). *Monográfico: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático*. Obtenido de Educacion.es: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

NETWORK-SEC. (7 de abril de 2015). *Gobierno TI: Network-Sec*. Obtenido de Network-Sec: http://www.network-sec.com/contenidos/Gobierno_TI.pdf

OVERTI. (7 de abril de 2015). *Home: Overti*. Obtenido de Overti: http://www.overti.es/iso-20000

PECB. (8 de abril de 2015). *Home: Pecb*. Obtenido de Pecb: http://pecb.org/iso22301es

Price watherhouse Coopers. (25 de enero de 2015). *Punto de vista: PricewatherhouseCoopers*. Obtenido de Price watherhouse Coopers: http://www.pwc,com/mx/es/publicaciones/archivo/2014-02-punto-vista.pdf

Romo, D., & Valarezo, J. (2015). *Análisis e implementación de la norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil.* Guayaquil: Universidad Politécnica Salesiana.

Secretaría Nacional de Administración Pública. (11 de febrero de 2011). *Acuerdo Ministerial 1002. Norma de Implementación y operación de Gobiernos por Resultados*. Obtenido de Secretaría Nacional de Administración Pública: http://blogs.espe.edu.ec/wp-content/uploads/2013/02/Norma-GPR2.pdf

Secretaría Nacional de la Administración Pública. (7 de enero de 2013). *Home: Secretaría Nacional de la Administración Pública*. Obtenido de Secretaría Nacional de la Administración Pública: http://www.administracionpublica.gob.ec/

Superintendencia de Bancos y Seguros. (5 de enero de 2014). *Descargas: Superintendencia de Bancos y Seguros*. Obtenido de Superintendencia de Bancos y Seguros: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf