PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Análisis de las metodologías de gestión de riesgos para garantizar la continuidad del negocio en el departamento de tecnologías de la información en la Corporación Nacional de Electricidad en Esmeraldas.

AUTOR:
Jesús David Bustos Lara

ASESOR:
Kléber Vera Tortorella

Mayo
del 2016

ÍNDICE

1. Resumen **2**

2. Abstract **3**

3. Justificación **4**

4. Objetivos **5**

5. Caso **6**

5.1 Antecedentes 6

5.2 Marco Teórico 7

5.2.1 Reconociendo riesgos 7

5.2.2 Gestión de riesgos 8

5.2.3 Componentes claves del riesgo 8

5.2.4 El proceso de administración de riesgos 11

5.2.5 Comprender el contexto empresarial 12

5.2.6 Gobierno de la seguridad: Frameworks, metodologías, estándares y guías 13

5.2.7 Eligiendo metodologías de gestión de riesgo 17

5.3 Metodología 17

5.4 Población y Muestra 18

5.5 Población 18

5.6 Muestra 19

5.7 Análisis de datos 19

6. Propuesta de intervención **20**

6.1 OCTAVE 25

6.2 OCTAVE-S 26

6.3 Ventajas 29

6.4 Desventajas 30

6.5 Implementación 30

6.5.1 Metas del proceso OCTAVE 35

6.5.2 Cronograma 36

6.6 Conclusiones 38

7. Referencias Bibliográficas **38**

8. Anexos **42**

1. Resumen

El siguiente estudio de caso realizado, analiza la cultura y los procedimientos sobre la seguridad de la información que se llevan a cabo en el departamento de TI de la Corporación Nacional de Electricidad Unidad de Negocio Esmeraldas, con la finalidad de identificar una metodología de gestión de riesgos que permitiese garantizar la continuidad del negocio.

Una metodología de gestión permite identificar el riesgo y estimar el impacto que tiene sobre los activos del sistema para tomar medidas de prevención y/o de mitigación.

Para el correcto desarrollo de la investigación se utilizó el método descriptivo-tecnológico. Como técnica de recolección de datos se utilizaron entrevistas para determinar la naturaleza de la gestión que manejan los miembros del departamento informático sobre los sistemas de información, además de entrevistas con la finalidad de describir los procesos que ellos utilizan para llevar a cabo la auditoría interna informática.

Posteriormente se eligió un grupo de metodologías usadas en la actualidad y se hizo un sondeo de su presencia en las investigaciones en el país. Luego, se comparó las diferentes metodologías de gestión de riesgos en base a factores encontrados en estudios previamente realizados. Como resultado de la comparación de las metodologías, OCTAVE-S fue considerada la metodología más adecuada para ser implementada en el departamento de TI de CNEL en Esmeraldas.

Para finalizar, se realizó una propuesta de intervención, en la cual se determinan los criterios que necesita cumplir el departamento de TI de la CNEL Unidad de Negocio Esmeraldas, para implementar OCTAVE-S como metodología de gestión de riesgos.

2. Abstract

The following case study analyzes the culture and information security procedures in the IT department of the National Electricity Corporation Esmeraldas Business Unit (CNEL), in order to identify a risk management methodology that ensures business continuity.

A risk management methodology allows us to identify risks, estimate it's impact to the system's assets exposed and take measures to prevent and / or mitigate them.

For the correct development of the research a descriptive-technological method was used. As a technique for data collection, interviews were held to determine the nature of management that the members of the IT department handle on information systems, as well as interviews in order to describe the processes they use to carry out internal IT auditing.

Later on, state-of-the-art methodologies were chosen and a survey of their presence in the research community in the country was made. Then, different risk management methodologies were compared based on factors found in previous analysis studies. As a result of the comparison, OCTAVE-S was considered the most appropriate methodology for CNEL's IT department in Esmeraldas.

Finally, a proposal for intervention was performed, determined under certain criteria needed to be met by the IT department of CNEL's Esmeraldas Business Unit in order to implement OCTAVE-S as a risk management methodology.

3. Justificación

Los recursos de tecnologías de información como cualquier activo en las organizaciones, se encuentran expuestos a riesgos, cuando estos se materializan, no solo degradan el recurso, sino que impactan en menor o mayor grado el cumplimiento de los objetivos (Jiménez,2009).

La gestión de riesgos ayuda a seleccionar y establecer medidas de seguridad apropiadas para controlar o eliminar riesgos identificados, asegurando la continuidad operacional de la organización. Además, permite un óptimo aprovechamiento de recursos, teniendo como resultado un aumento de ganancias y la reducción de pérdidas, haciendo que este proceso añada valor a las operaciones de la institución.

CNEL EP tiene como objetivo brindar el servicio público de distribución y comercialización de energía eléctrica para generar bienestar a los habitantes de todas las provincias costeras de Ecuador y la provincia de Sucumbíos, contribuyendo al desarrollo del país, con talento humano comprometido, tecnología de punta, innovación y respeto al ambiente.

Con el antecedente indicado, el presente estudio de caso tiene como finalidad realizar un análisis de metodologías para la gestión del riesgo de los sistemas informáticos de la CNEL EP Unidad de Negocio Esmeraldas. A través del resultado del estudio, se podrá determinar la mejor metodología que deberá aplicarse a los sistemas de información, con lo cual se contribuirá a que la Corporación Nacional de Electricidad posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información, identificando las áreas críticas que requieran un mayor control y que esto resulte en un mejor servicio público para la comunidad esmeraldeña.

4. Objetivos

OBJETIVO GENERAL:

Analizar las metodologías de gestión de riesgos para garantizar la continuidad del negocio en el departamento de tecnologías de la información en la Corporación Nacional de Electricidad en Esmeraldas.

OBJETIVOS ESPECÍFICOS:

- Examinar la metodología de gestión de riesgo existente en la empresa.
- Conocer el proceso de auditoría informática que realiza el departamento de TI con el fin de conocer sobre su expectativa sobre el riesgo.
- Seleccionar una metodología que mejor se adapte a las necesidades de CNEL para mitigar los riesgos inherentes.
- Elaborar una propuesta que permita aplicar la metodología para optimizar la gestión de riesgo en CNEL.

5. Caso

5.1. Antecedentes

El análisis de riesgos dentro del país tiene una gran importancia en el sector público. La Controlaría General del Estado de Ecuador se encarga de auditar y cuidar que los recursos del Estado se usen adecuadamente y que los objetivos estratégicos de las Instituciones Públicas se cumplan.

La Contraloría cuenta con un apartado sobre Tecnologías de la Información en la sección 410 dentro de su documento "Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos".

Estas normas de control interno que recogen la utilización del marco integrado de control interno emitido por el Comité de Organizaciones que patrocina la Comisión Treadway (COSO) (Ministerio del Interior, 2014); plantean cinco componentes interrelacionados e integrados al proceso de administración (Administración Financiera, Administración del Talento Humano, Administración de Proyectos, Gestión Ambiental y Tecnología de la Información), con la finalidad de proporcionar un alineamiento entre las prácticas del negocio y la tecnología, además de brindar una guía para la gestión corporativa y que esta se relacione con el reglamento gubernamental. (Ver Anexo 1)

La seguridad de la información se ha convertido en una necesidad creciente por las múltiples formas de ataque que se van desarrollando día tras día, y muchos son los trabajos que abordan desde diferentes tópicos la salvaguarda de los datos, así se tienen diferentes trabajos de investigación que se mencionan a continuación:

En la investigación de Padilla (2012) para el Análisis y Gestión de Riesgos Informáticos del Gobierno Provincial de Tungurahua, recomienda la metodología de gestión de riesgo MAGERIT como la más adecuada para el control de la información y de los activos físicos de la organización.

En la investigación de Gallardo y Jácome (2009) hecha para analizar los riesgos y elaborar un plan de contingencia para la Empresa Eléctrica Quito S.A, se seleccionó la metodología OCTAVE por su popularidad, análisis exhaustivo y comprensión realista de la organización.

5.2. Marco Teórico

5.2.1. Reconociendo riesgos

Qué es considerado riesgo y cómo debe ser descrito, depende del contexto de la organización que enfrenta ese riesgo, y de los prejuicios del individuo que lo evalúa (National Technical Authority for Information Assurance, 2015).

Según la normativa ISO/IEC 27005:2008 (2008) el riesgo se define como "el potencial que tiene una determinada amenaza para explotar las vulnerabilidades de un activo o grupo de activos y por consiguiente causar daño a la organización".

Las organizaciones no pueden desarrollarse sin tomar riesgos. El riesgo tecnológico y de información no se trata solamente de mitigación y evitación; la búsqueda y aceptación de riesgos crea oportunidades y pueden ayudar a conseguir los objetivos del negocio.

Habiendo reconocido este amplio significado, se usará la palabra 'riesgo' para describir el potencial para el daño a la seguridad como resultado del uso de la tecnología e información con el fin de alcanzar objetivos estratégicos (National Technical Authority for Information Assurance, 2015).

Es importante no pensar solamente en el riesgo en el contexto de confidencialidad, integridad y disponibilidad de la tecnología y la información. Además de estas, otras cosas sobre las que la organización se preocupa (como su reputación) pueden estar en riesgo y también deben ser tomadas en cuenta (National Technical Authority for Information Assurance, 2015).

5.2.2. Gestión de riesgos

Según ISACA (2006), la gestión de riesgos es el proceso de identificar vulnerabilidades y amenazas a las fuentes de información usadas por una organización para alcanzar objetivos estratégicos, y decidir qué medidas tomar, si se necesitan tomarlas para reducir el riesgo hasta un nivel aceptable, basadas en el valor de la fuente de información para la organización. El propósito de la gestión de riesgos es ayudar a la organización a protegerse a sí misma, y que confíe que la tecnología e información que usa es suficientemente segura para que cumpla con sus necesidades.

Cuando las acciones y decisiones de la gestión de riesgos afectan múltiples organizaciones en un contexto empresarial, algún nivel de coordinación de gestión de riesgo será requerido. Puesto que las necesidades de la organización, las amenazas que enfrenta y la vulnerabilidad de la tecnología de la información cambian con el tiempo, la gestión de riesgos necesita darse a través del ciclo de vida de un sistema o servicio, informado de una vista realista de los riesgos y un entendimiento claro de la organización y sus objetivos.

El riesgo de la tecnología e información es sólo una parte del riesgo de negocio que la organización necesita manejar. Por este motivo, debería encajar con el resto de las actividades de gestión de riesgos del negocio tomadas por la organización.

5.2.3. Componentes clave del riesgo

Las evaluaciones de riesgos tienen entradas y salidas. Los insumos fundamentales a tener en cuenta en una evaluación de riesgos son la amenaza, la vulnerabilidad y el impacto. El riesgo se realiza como consecuencia de estas entradas, aunque algunos enfoques de evaluación de riesgos incluyen otros insumos (como la probabilidad y el valor de los

activos). Independientemente del método de evaluación de riesgos utilizado, todas las entradas y salidas deben ser comprensible y significativa en el contexto de la empresa y lo que está tratando de lograr. (National Technical Authority for Information Assurance, 2015)

Amenaza

Una amenaza describe la fuente de un riesgo que se está identificando. Las amenazas a los sistemas y servicios incluyen personas que buscarían hacer daño al negocio a través de la tecnología, y peligros como desastres ambientales y accidentes. Algunas de las amenazas que una organización puede enfrentar están fuera del control de la organización; sólo pueden utilizar el conocimiento de amenazas para facilitar la priorización de riesgos (National Technical Authority for Information Assurance, 2015).

Vulnerabilidad

La vulnerabilidad es una debilidad que puede ser explotada por una amenaza provocando un impacto. Un sistema o servicio podría verse comprometido por la explotación de las vulnerabilidades de las personas, lugares, procesos o tecnología (National Technical Authority for Information Assurance, 2015).

Al evaluar sus riesgos, las organizaciones deben asegurarse de que tienen una comprensión clara y realista de dónde y cómo sus sistemas y servicios son vulnerables. Mientras que las organizaciones no pueden controlar las amenazas que enfrentan, pueden reducir sus vulnerabilidades (National Technical Authority for Information Assurance, 2015).

Impacto

El impacto describe las consecuencias de un riesgo detectado. Para permitir la evaluación de riesgos y el establecimiento de prioridades, el impacto debe especificar el efecto negativo que la realización de un riesgo implicaría.

Esto debe incluir las pérdidas esperadas (por ejemplo, pérdidas financieras y de reputación), así como los objetivos de negocio que no serían alcanzables como resultado del impacto. Las organizaciones pueden ejercer control sobre el posible impacto negativo en la ocurrencia de un incidente debido al riesgo, y deben planificar para que esto suceda.

Otras entradas

Algunos métodos de evaluación de riesgos también consideran valores de probabilidad y de activos como componentes del riesgo y entradas a las evaluaciones.

La probabilidad calcula qué tan probable es que se produzca una amenaza. Puede ser capturada mediante el examen de los registros históricos de los compromisos para estimar cómo se repite la historia. Algunos métodos se basan en la probabilidad para ayudar a determinar la vulnerabilidad. Hay que tener en cuenta que las métricas de sucesos pasados no son necesariamente un indicador útil de lo que sucederá en el futuro.

El valor de los activos se utiliza para proporcionar una comprensión de que sistemas, servicios, información u otros activos le importan realmente a la organización. Esta visión les proporciona a las organizaciones una vista de lo que realmente quieren proteger. La valoración de los activos es un factor clave para determinar el impacto de entrada para los propósitos de evaluación de riesgos (National Technical Authority for Information Assurance, 2015).

Salida de evaluación de riesgos

Independientemente del método de evaluación de riesgos utilizado, la salida debe ser significativa, comprensible, realista, en contexto para que informe decisiones de gestión de riesgos y que no pueda interpretarse de diferentes maneras por diferentes personas.

El nivel y el tipo de detalle proporcionado por la salida (p. ej., técnica o no) dependerán de a quién va dirigida la evaluación del riesgo y que decisión para la gestión de riesgos se quiere informar.

5.2.4. El proceso de administración de riesgos

Jiménez (2008) expone que, en los diferentes enfoques o metodologías existentes para la administración de riesgos, es común encontrar una serie de tareas o fases principales, que se pueden definir como:

• Planificación del riesgo, define las acciones necesarias para crear un plan de riesgo que incluya la metodología a utilizar, los roles, las responsabilidades y el presupuesto para implementar el plan y los cronogramas asociados.

• Identificación del riesgo, considera la determinación de elementos de riesgos potenciales mediante la utilización de algún método consistente y estructurado, como la tormenta de ideas, técnica Delphi, entrevistas o FODA. Lo importante en esta fase es acceder a la experiencia del propietario o usuario de la actividad, función o proceso en análisis.

• Análisis, los riesgos se determinan en términos de su probabilidad de ocurrencia e impacto (consecuencia). El análisis debería considerar el rango de consecuencias potenciales y que tan probable es que ocurran esas ocurrencias, se obtiene una lista priorizada de los mismos bajo las prioridades de la administración.

• Planificación de la respuesta al riesgo es el proceso para desarrollar opciones y determinar acciones para reducir las amenazas. Incluye la identificación y la asignación de individuos para tomar la responsabilidad de cada respuesta por cada riesgo. Este proceso asegura que los riesgos identificados sean tratados correctamente.

• Seguimiento y control pretende no perder de vista los riesgos identificados. Supervisar los riesgos residuales e identificar nuevos, asegurar la ejecución de los planes y de evaluar su eficacia en la reducción de riesgo (Jiménez,2008).

5.2.5. Comprender el contexto empresarial

Tomar riesgos es una parte necesaria de hacer negocios con el fin de crear oportunidades y ayudar a cumplir los objetivos de negocio. Las organizaciones siempre deben ser conscientes de los riesgos que están tomando para alcanzar sus objetivos (National Technical Authority for Information Assurance, 2015).

Para asegurar resultados significativos, las organizaciones necesitan para proporcionar un contexto en el que se lleva a cabo la gestión de riesgos y la evaluación de riesgos. De acuerdo a National Technical Authority for Information Assurance (2015), este contexto puede ajustarse respondiendo a las siguientes preguntas:

¿Qué es lo que la organización está tratando de lograr, y qué es lo que realmente importa?

¿Cuáles son los activos del negocio involucrados (por ejemplo, sistemas, servicios, información y otros activos de la empresa, tales como la reputación), y ¿para qué sirven a la organización?

¿Qué riesgos está la organización preparada / no preparada para llevar con esos activos para lograr sus objetivos?

¿Existen requisitos legales y regulatorios externos que deben tenerse en cuenta?

¿Hay una tercera gestión de riesgos o consideraciones contractuales que tener en cuenta?

¿Qué recompensas pueden ser ganadas por tomar riesgos?

¿Qué estructura de gobierno tendrá la organización para apoyar la toma de decisiones de gestión de riesgos?

Los responsables de la toma de decisiones de gestión de riesgos deberían contribuir y estar de acuerdo con la definición de este contexto.

5.2.6. Gobierno de la seguridad: Frameworks, Estándares, Guías y Metodologías

Un estándar es un conjunto de reglas bastamente reconocidas o implementadas (especialmente por su excelencia) que controlan como la gente desarrolla y gestiona materiales, productos, servicios, tecnologías, tareas, procesos y sistemas (Kiran, Reddy y Lakshmi,2013).

- Estándares como el ISO/IEC 27001 y 27002 no definen pasos detallados para el reconocimiento de riesgos, si se quieren usar estos estándares hay que definir métodos propios de evaluación de seguridad o se pueden usar métodos desarrollados por otras organizaciones.

- ISO 27001 se centra en las normas de seguridad de la información, y fue actualizado por última vez en el año 2013. En él se describe una serie de directrices sobre mejores prácticas para asegurar que los datos electrónicos se mantengan de una manera segura (Alfafara,2009).

Los marcos de trabajo o *"*frameworks*"* existen para ayudar a los negocios y organizaciones a tener buenas prácticas en sus campos específicos, a tener una buena gestión y fueron creados para crear compatibilidad entre los procesos de los negocios y

los recursos tecnológicos, también se usan con fines regulatorios para satisfacer las necesidades específicas del negocio o necesidades del gobierno.

Estos marcos incentivan el uso de metodologías comprobadas, ayudan al cumplimiento de estándares relevantes, y pueden ayudar a reducir riesgos y costos operativos (Collaboris, s.f)

Los principales marcos de trabajo que se encuentran en la actualidad son:

- **COSO**

Ayuda a las organizaciones a diseñar e implementar el control interno a la vista de muchos cambios en los negocios y entornos operativos, a ampliar la aplicación del control interno en el tratamiento de las operaciones y la presentación de objetivos y aclarar los requisitos para la determinación lo que constituye un control interno efectivo. (COSO,2013).

De acuerdo al marco COSO, el control interno consta de cinco componentes relacionados entre sí; que estarán integrados en el proceso de dirección.

Los componentes son:

1. Ambiente de Control. La organización debe establecer un entorno que permita el estímulo y produzca influencia en la actividad del recurso humano respecto al control de sus actividades (Cuellar,2013).
2. Evaluación de Riesgos. La organización al establecer su misión y sus objetivos debe identificar y analizar los factores de riesgo que puedan amenazar el cumplimiento de los mismos (Cuellar,2013).
3. Actividades de Control. Las actividades de una organización se manifiestan en las políticas, sistemas y procedimientos, siendo realizadas por el recurso humano que integra la entidad (Cuellar,2013).
4. Información y Comunicación. La entidad debe contar con sistemas de información eficientes orientados a producir informes sobre la gestión, la realidad financiera y

el cumplimiento de la normatividad para así lograr su manejo y control (Cuellar,2013).

5. Supervisión y Monitoreo. Planeado e implementado un sistema de Control Interno, se debe vigilar constantemente para observar los resultados obtenidos por el mismo (Cuellar,2013).

- **COBIT**

COBIT es un marco de gobierno dirigido al cumplimiento normativo y gestión de riesgos. Ahora, en su quinta edición, que abarca áreas como la auditoría y aseguramiento y la gobernanza de los sistemas de TI de la empresa.

Marco de trabajo: Organiza los objetivos de gobierno de TI y las buenas prácticas por dominios de TI y procesos, y los vincula con los requisitos de negocio.

Descripciones de procesos: Un modelo de procesos de referencia y lenguaje común para todos los miembros de una organización. Los procesos se asignan a las áreas de responsabilidad de planear, construir, ejecutar y controlar.

Objetivos de control: Proporcionan un conjunto completo de requisitos de alto nivel para ser considerados por la administración para el control efectivo de cada proceso de TI.

Directrices de gestión: Ayuda a asignar responsabilidad, ponerse de acuerdo sobre los objetivos, medir el rendimiento, e ilustrar la interrelación con otros procesos.

Modelos de madurez: Evalúan la madurez, la capacidad de cada proceso y ayuda a hacer frente a las faltas.

- **ITIL**

ITIL se centra en cómo los servicios de TI deben utilizarse para respaldar las metas y objetivos de negocio. Originalmente desarrollado por el gobierno del Reino Unido en la década de 1980 para estandarizar su creciente uso de TI, ahora es utilizado por instituciones y empresas de todos los tamaños y formas.

Según OSIATIS (s.f.), el Ciclo de Vida del Servicio consta de cinco fases que se corresponden con los nuevos libros de ITIL:

1. **Estrategia del Servicio**: propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico.
2. **Diseño del Servicio**: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
3. **Transición del Servicio**: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
4. **Operación del Servicio**: cubre las mejores prácticas para la gestión del día a día en la operación del servicio.
5. **Mejora Continua del Servicio**: proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a traces de un diseño, transición y operación del servicio optimizado.

Las guías son consejos o instrucciones dadas a fin de orientar o dirigir una acción. (Kiran, Reddy y Lakshmi,2013).

Una metodología es una construcción enfocada que define practicas específicas, procedimientos, y reglas para la implementación o ejecución de una tarea específica o función (Tomhave, 2006).

5.2.7. Eligiendo metodologías de gestión de riesgo de TI

Al escoger un marco de gestión y metodología de evaluación de riesgos, una organización debe asegurarse de que se ajuste a sus propósitos.

Algunas consideraciones pueden incluir:

- Costo
- Alcance del proyecto
- Garantía de que los recursos requeridos son proporcionados y sostenibles
- Carácter comercial que podría restringir su uso

Hay que tener en cuenta que otros métodos diferentes a los mencionados aquí pueden resultar una mejor opción, en función de las circunstancias particulares de las necesidades de los negocios y tecnología. Utilizar una única metodología puede no satisfacer sus necesidades; estas consideraciones no son las únicas y es posible que desee utilizar un enfoque híbrido o desarrollar su propio (National Technical Authority for Information Assurance, 2015).

5.3. Metodología

Esta investigación, se desarrolló en un marco de investigación tecnológica que hizo uso del conocimiento científico y tecnológico, para modificar el proceso productivo de la CNEL EP Unidad de Negocio Esmeraldas.

Como parte del proceso ingenieril se procede a una adaptación intencionada de medios para alcanzar un fin preconcebido superador de una situación inicial dada, y esto constituye una parte esencial de la ingeniería (Dean,2002).

De acuerdo al nivel de profundidad de la investigación esta será del tipo descriptiva proporcionando un perfil de la condición de la empresa en la actualidad para comprender el comportamiento de CNEL en relación a la gestión de riesgos tecnológicos.

De acuerdo a la naturaleza de datos y a las técnicas de recopilación de los datos (entrevista), la investigación realizada fue cualitativa, ya que no se pretende analizar todos los procesos de la empresa sino una muestra de ellos; además de conocer la opinión y cultura de la empresa en cuanto a tolerancia a riesgos y objetivos de gestión para dar un enfoque a la elección de la metodología. Estos resultados no podrán ser generalizados debido a su especificidad, otra razón por la elección de este tipo de investigación.

La investigación cualitativa se centra en la recopilación de información principalmente verbal en lugar de mediciones. Luego, la información obtenida es analizada de una manera interpretativa, subjetiva, impresionista o incluso diagnóstica (Explorable.com, 2009)

Para conocer sobre el estado de las metodologías de gestión de riesgo tecnológico que se están aplicando actualmente en el Departamento Técnico de CNEL se procedió a realizar entrevistas a los miembros del equipo técnico. También se emplearon fichas de evaluación de riesgos proporcionadas gratuitamente por la Universidad de Connecticut desde su sitio web.

La presente investigación tuvo como base científica distintos tipos de documentos accedidos mediante Internet como, libros digitales, tesis de grado, artículos científicos, estudios de caso y bases de conocimiento gubernamentales, las mismas que fueron utilizadas para redactar el marco teórico y los antecedentes, y que además fueron referenciadas haciendo uso de las normas APA 6ta Edición.

5.4. Población y Muestra

5.4.1. Población

La recolección de los datos se realizó en la Corporación Nacional de Electricidad Unidad de Negocio Esmeraldas, durante el periodo académico 2015-2016. La población está conformada por el jefe departamental, y equipo de desarrollo del departamento de TIC.

5.4.2. Muestra

Los administradores del departamento de TI de CNEL Unidad de Negocio en la ciudad de Esmeraldas son 3 personas. Peor este motivo no se aplicó la técnica de muestreo y se procedió a realizar la encuesta al total de población.

5.5. Análisis de los datos

Se realizó entrevistas **(Ver Anexo 2)** a los miembros del departamento de sistemas informáticos de CNEL Unidad de Negocio Esmeraldas, incluidos están el Jefe del departamento y un analista de sistemas; sus respuestas en cuantos a la cultura organizacional enfocada a la seguridad de la información fueron las siguientes:

- Existen 120 funcionarios administrativos.
- No se usa ninguna metodología y los procesos de evaluación se hacen de una forma general, no minuciosa. Se desea aplicar una metodología.
- El departamento de TI considera sus riesgos relativamente bajos.
- La Oficina Central se le ha proporcionado a la Unidad procedimientos sobre como respaldar información, solicitar información, procesos de garantía.
- Se prioriza el software libre y software de código abierto para evitar costos.
- No se desea la cuantificación del riesgo.
- Se hace una auditoría anual con la ayuda de un software llamado OCS Inventory, y junto al conjunto de políticas forma parte de los procesos de manejo de riesgos.
- La auditoría llevada es externa, llevada por la Contraloría General del Estado, dura aproximadamente 3 semanas con la ayuda de información proporcionada por el departamento de TI como registros de servidores, políticas y funciones de sus integrantes. Por este motivo este proceso no es controlado por CNEL.
- Sólo existe 1 entidad auditora para CNEL.
- No ha habido irregularidades por las que la Contraloría deba intervenir.
- La última observación en la auditoría a CNEL Esmeraldas se dio por una inadecuada implementación del centro de datos. Se convocará a un concurso para empezar el proyecto de construcción en el año 2017.

6. Propuesta de intervención

El análisis de los datos recogidos anteriormente determina que CNEL no cuenta con una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera informal, se encontró la necesidad de definir y posteriormente implementar una metodología de gestión de riesgos tecnológicos para asegurar la continuidad del negocio en CNEL. Se determinó aplicar un proceso que permita encontrar la metodología más adecuada que cumpla con los requerimientos del departamento técnico.

Como primer criterio de selección se tomó un conjunto de investigaciones realizadas en Ecuador para averiguar el estado del arte en cuanto a evaluación a riesgos, se tomó 11 investigaciones de pregrado y posgrado para elegir un subconjunto de metodologías para evaluar. Adicionalmente, se tomó un grupo de 9 metodologías a ser sondeadas, las cuales fueron inicialmente identificadas en el análisis comparativo de Kiran, Reddy y Lakshmi (2013).

La muestra de investigaciones contiene soluciones para la gestión de riesgos en empresas e instituciones públicas y privadas del sector gubernamental, educativo superior, automotriz, y microempresas; particularmente los trabajos de Gallardo y Jácome (2013) y Granda (2011) tratan la gestión de riesgos en la Empresa Eléctrica Quito S.A y la Empresa Eléctrica Regional Centro Sur.

PRESENCIA DE METODOLOGÍAS DE GESTIÓN DE RIESGO DE TI EN ECUADOR									
INVESTIGACIONES	OCTAVE	MAGERIT	MEHARI	IRAM	IT-GRUNDSCHUTZ	EBIOS	CRAMM	MARION	MIGRA
Gallardo y Jácome (2011)	x	x	x						
Aucancela (2012)	x	x		x			x		
Gaona (2013)		x							
Reyes (2014)	x	x	x						
Paredes y Vega (2011)		x							
Sangoluisa (2015)	x	x							
Moncayo (2014)	x	x							
Granda (2011)	x	x	x						
Mera (2015)	x	x							
Conza y Medrano (2013)	x	x	x				x		
Jara (2011)	x	x	x		x	x	x		

Tabla I. Tabla de presencia de metodologías en Ecuador

La tabla anterior muestra una comparación de diferentes metodologías. Cada vez que una metodología es mencionada por un autor, recibe una marca y 1 punto. Se obtuvieron 9 menciones de OCTAVE, 11 de MAGERIT, 5 de MEHARI, 1 de IRAM, 1 de IT-GRUNDSCHUTZ, 1 de EBIOS, 3 de CRAMM, 0 de MARION, y 0 de MIGRA.

Entre las metodologías más relevantes del mercado en Ecuador se pudieron encontrar las siguientes:

- OCTAVE
- MAGERIT

- MEHARI
- CRAMM
- EBIOS

Para determinar la metodología que se acople a cubrir los requerimientos del departamento de TI de CNEL Unidad de Negocio Esmeraldas, en primer lugar, se deben establecer criterios de presencia con la finalidad de reducir la lista de las metodologías anteriormente expuestas a un número de una, y así lograr establecer la más adecuada para el departamento de tecnología de CNEL. Los criterios de presencia seleccionados para la evaluación de las metodologías son los siguientes:

- Costo
- Tipo de Análisis
- Disponibilidad de documentación
- Herramientas (si el modelo provee herramientas de apoyo y como las podemos obtener)
- Seguimiento de estándares de calidad.
- Tamaño de la organización.

Una vez expuestos los criterios de presencia, se procedió con la evaluación de las metodologías de gestión de riesgos tal y como lo describe (Kiran, Reddy y Lakshmi, 2013) en su investigación, obteniendo como resultado la siguiente tabla:

	OCTAVE	MAGERIT	MEHARI	CRAMM	EBIOS
Tipo de análisis	Cualitativo	Cuantitativo y Cualitativo	Cualitativo	Cualitativo	Cualitativo
Enfoque	Estilo de Workshops, ambiente colaborativo y apoyado con guías, hojas de trabajo, y cuestionarios, los cuales son incluidos en el método.	Más de una técnica para calcular el riesgo	Basa su análisis en formulas, parámetros, y una base de conocimiento ; Auditorías son llevadas a cabo para identificar vulnerabilidades potenciales.	Usa expertos y software para calcular los riesgos para cada grupo de activos contra las amenazas a las que es vulnerable en una escala de 1 a 7, utilizando una matriz de riesgo.	Autoevaluación y discusión en un grupo mixto (manager, IT y usuarios)
Costo	Uso libre o gratuito	Licencia Comercial	Uso libre o gratuito	Licencia Comercial	Uso libre o gratuito
Herramientas	Sin herramientas pero con documentación de soporte	EAR/PILAR ($250-$2000)	Mehari Basic Tool (Hoja de Excel gratis). Risicare (Licencia Comercial)	CRAMM Express ($2000) CRAMM Expert ($4441)	EBIOS Tool
Estándares	N/A	ISO/IEC 13335 17799 15408 27001	ISO/IEC 27001 13335	ISO/IEC 27001	ISO/IEC 27001, 13335, 15408, 17799
Última revisión	2011	2013	2010	2005	1995

Tabla II. Comparativa de metodologías de gestión de riesgos.

Actualmente existe una gran variedad de metodologías de gestión de riesgos, cada una de ellas con cualidades y enfoques diferentes, pero siempre manteniendo la finalidad de prevenir desastres y mitigarlos. En la Tabla II se muestran las metodologías como cualitativas (involucrando cifras y cálculos en pérdidas monetarias) o cuantitativas (basadas en evaluaciones subjetivas de probabilidad y consecuencia de cualquier amenaza

que esté ocurriendo en contra de un activo de información).

El análisis de riesgos cuantitativo es frecuentemente usado en la banca y el sector de las aseguradoras donde el riesgo puede ser cuantificado. Sin embargo, en el campo de TI, donde es imposible calcular cuantas veces el servidor puede ser hackeado, o cuantas veces el sistema se va a colgar resulta en algo impráctico; haciendo el análisis cualitativo una opción factible.

El problema en usar una metodología como EBIOS o Mehari es el esfuerzo empleado en recolectar la información siendo metodologías muy exhaustivas. Esto presenta una interrogante hacia la metodología en cuanto al retorno de inversión (ROI). Si se invierte mucho tiempo en conseguir los resultados, comparados al valor de sus sistemas de información entonces se debe pensar con cuidado.

Los métodos cuantitativos son buenos, pero requieren una gran inversión y pueden dar resultados engañosos si no se tiene cuidado con las medidas que se establecen (p ej. la probabilidad de riesgo es esencial, pero a veces es muy difícil de evaluar). Los métodos cualitativos a veces son muy vagos. Ambos pueden dar un sentimiento falso de estar suficientemente protegido.

El enfoque de las metodologías varía entre modelos; utilizando diferentes técnicas y procesos para su implementación, estas pueden hacer uso de evaluadores externos o pueden realizarse internamente en la organización, pueden usar una base de conocimiento o la experiencia de experto certificado; técnicas como las entrevistas, talleres, y listas de comprobación diferencian el sentido que la evaluación de riesgos va a tener.

Otro criterio de comparación, especifica la naturaleza comercial de las metodologías estudiadas. El costo de emplear, así como el costo de la compra de la metodología, sus herramientas y documentación deben ser consideradas. El tiempo invertido en la recopilación de los datos de seguridad, y el tiempo dedicado a la realización de estimaciones complejas (por ejemplo, las estimaciones financieras de los datos de seguridad que son difíciles de cuantificar financieramente), contribuyen al costo de la utilización de un método.

Así se puede excluir la metodología si no está disponible por ser difícil de conseguir al ser privada o ser muy costosa para la empresa. También se especifica si la herramienta de apoyo está en forma de software, plantillas de trabajo o si es inexistente.

Se revisan los estándares a los que se adhieren las metodologías dentro de sus procesos, aquellas que no sigan un estándar podrían ser flexibles para que sean compatibles con los requerimientos de la organización. Aunque estos estándares proveen métricas de calidad, algunas organizaciones pueden creer que seguirlos, no es el factor más determinante que justifique su éxito operacional en seguridad de la información, por otro lado, otras organizaciones pueden estar obligadas a seguir un estándar debido a regulaciones por la administración o el gobierno.

El criterio de última revisión permite conocer cuando la metodología ha sido actualizada o revisada, esto permite excluir a las metodologías que hayan sido descontinuadas, que estén obsoletas o que no hayan sido actualizadas en más de una década.

Con estos antecedentes se ha propuesto que se implemente la metodología **OCTAVE-S**, ya que esta metodología dadas sus características, componentes, equipo de trabajo y resultados es el que mejor se adapta al tamaño, necesidades, perspectivas y resultados que requiere esta empresa. OCTAVE es una metodología sencilla, de fácil acceso y gratuita con un enfoque de gestión interna y que puede encargarse de los objetivos de la empresa y los activos como Unidad de Negocio y Corporación.

6.1. OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología desarrollada por la institución de ingeniería de software de la Universidad de Carnegie Mellon, se utiliza para definir una evaluación estratégica basada en el riesgo y una técnica de planificación de seguridad que incorpora el análisis de comportamiento de la organización y las debilidades de la tecnología. OCTAVE es un analizador de componentes importantes que pueden construir un equipo interno de la empresa en sí que tiene las habilidades técnicas y capacidad de organización relacionados a la práctica de negocio.

OCTAVE es un enfoque auto dirigido, lo que significa que las personas de una organización asumen la responsabilidad de establecer la estrategia de seguridad de la organización.

Puntos fuertes de OCTAVE:

- Evaluación de la organización frente a una evaluación del Sistema
- Centrarse en las prácticas de seguridad frente a centrarse en la tecnología
- Temas estratégicos frente a los tácticos
- Autodirección vs dirección de expertos.

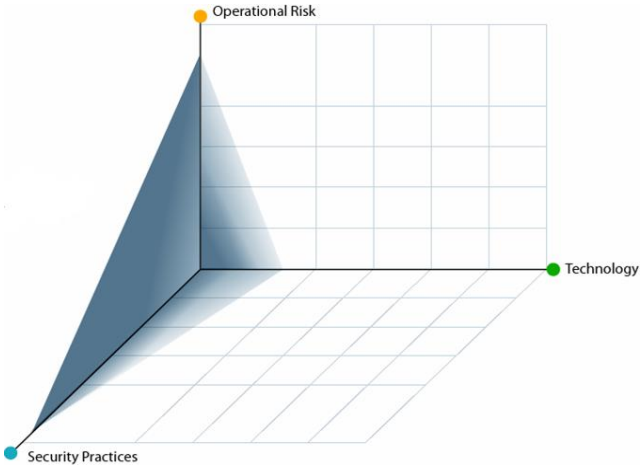

Figura 1. OCTAVE se centra en las prácticas de seguridad y el riesgo operacional (Cert,2005) Obtenido de *www.cert.org*

6.2. OCTAVE-S

Este método creado en el 2005 surge debido a la necesidad de organizaciones más pequeñas con aproximadamente 100 personas o menos. Se basa en el método OCTAVE, pero está adaptado a los limitados medios y restricciones únicas de las pequeñas organizaciones; OCTAVE-S utiliza un proceso simplificado y más hojas de trabajo diferentes, pero produce el mismo tipo de resultados, lo cual se acomoda a las necesidades de la Unidad de Negocio Esmeraldas de CNEL.

Cada método de OCTAVE-S es único, ya que se adapta al entorno de riesgos de la organización, sus objetivos de seguridad, la capacidad de recuperación y el nivel de habilidad del personal de la empresa. OCTAVE se centra en las amenazas y riesgos de seguridad de información, pero mira más allá del nivel del sistema ya que se enfoca en las personas y los procesos (Páez, 2013).

Fig. 2 Proceso OCTAVE (Cequeda, s.f)
Obtenido de: https://seguridadinformaticaufps.wikispaces.com/

El método OCTAVE-S cuenta con 3 fases las cuales son:

1. Construcción de perfiles de amenazas basados en los activos (Páez,2013).

Esta fase cuenta con los siguientes procesos:

- Identificar la información organizacional
- Crear perfiles de amenazas.

Para los que se desarrollan las siguientes actividades:

- Establecer el impacto de los criterios de la evaluación.
- Identificar activos organizaciones.

- Evaluar prácticas de seguridad organizacionales
- Seleccionar activos críticos.
- Identificar requerimientos de seguridad
- Identificar amenazas a los activos críticos.

2.Identificación de las vulnerabilidades de la infraestructura (Páez,2013).

Cuenta con un solo proceso en el que se examina la infraestructura computacional en relación a los activos críticos (Páez,2013) para lo que se definen las siguientes actividades:

- Examinar rutas de acceso.
- Analizar los procesos relacionados con tecnología.

3.Desarrollo de estrategia y planes de seguridad.

En la Fase Tres se desarrollan planes y estrategias de seguridad a través de los siguientes procesos: identificar y analizar los riesgos y desarrollar estrategias y planes de mitigación (Páez,2013).

Se cuenta con las siguientes actividades:

- Evaluar el impacto de las amenazas.
- Establecer criterios basados en la frecuencia.
- Evaluar probabilidades de amenaza.
- Describir la estrategia de protección actual.
- Desarrollar un plan de mitigación.
- Identificar cambios a la estrategia de protección e identificar siguientes pasos.

Las dos principales diferencias en esta versión de OCTAVE que coinciden con la situación de la empresa son:

1. OCTAVE-S requiere un pequeño equipo de 3-5 personas que entienden la amplitud y profundidad de la empresa. Esta versión no comienza con el conocimiento formal sino con la obtención de talleres para recopilar información sobre los elementos importantes, los requisitos de seguridad, las amenazas y las prácticas de seguridad. El supuesto es que el equipo de análisis de esta información ya se conoce.

2. OCTAVE-S incluye sólo una exploración limitada de la infraestructura informática. Las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad.

La documentación incluye hojas de trabajo y orientaciones para cada actividad, así como una introducción, la guía de preparación, y un ejemplo completo. No se incluye aún la adaptación de orientación a reuniones o de información.

6.3. Ventajas

- Flexible: Cada método se puede adaptar al entorno de riesgos que es único para su organización, los objetivos de seguridad y capacidad de recuperación y el nivel de habilidad (Páez, 2013).

- Los escenarios de los talleres abarcan una amplia gama de posibles incidentes de seguridad, lo que ayuda a prever y planear distintas acciones y medidas de seguridad en caso de que se presente alguna amenaza (Páez, 2013).

6.4. Desventajas

- La metodología fallará si las personas involucradas no tienen un amplio conocimiento de los procesos operativos y de seguridad de la organización.
- No permite modelar matemáticamente el riesgo (no es de interés de la Unidad de Negocio).

6.5. Implementación

El enfoque inicial de OCTAVE es preparar para la evaluación. De acuerdo al Volumen 2 de la guía de implementación de OCTAVE hecha por CERT (2005), se pueden consideran cuatro puntos como factores clave del éxito:

1. Conseguir el patrocinio de la alta dirección (Administrador). Este es el factor de éxito por excelencia para las evaluaciones de riesgo de seguridad de la información. Si los directivos no apoyan el proceso, el personal de apoyo para la evaluación se disipará rápidamente.

   Se aconseja llevar a cabo una evaluación limitada. Una evaluación limitada se centra en un área de la organización (a menudo en un solo activo). El equipo de análisis realiza una evaluación de alcance limitado y presenta los resultados a los altos directivos. En el caso de CNEL, la evaluación inicial podría darse en el área comercial o tecnológica. Este enfoque permite a los gerentes de alto nivel ver lo que los resultados de la evaluación y pueden ser una buena manera de conseguir que se interesen en la metodología.

2. Selección del equipo de análisis. El equipo de análisis se encarga de gestionar el proceso y análisis de la información. Los miembros del equipo necesitan tener suficientes habilidades y entrenamiento para conducir la evaluación y para saber cuándo hay que aumentar sus conocimientos y

habilidades mediante la inclusión de personas adicionales para una o más actividades.

Se deben incluir entre tres y cinco personas que representen el conocimiento del negocio, su misión, los procesos y visión de TI, que tengan buena comunicación y compromiso.

Entre sus actividades se incluyen:

• Programar actividades OCTAVE-S
• Conducir las actividades de evaluación
• Reunir, analizar y mantener datos de evaluación durante el proceso.
• Coordinar logísticas (1 persona)

Si el equipo de análisis decide empezar sin formación, hay algunas cosas que se pueden hacer para facilitar el proceso de aprendizaje. En primer lugar, todos los miembros del equipo deben pasar tiempo leyendo sobre OCTAVE-S y discutirlo entre sí. El equipo debería ejecutar un piloto mediante la selección de un activo que los miembros del equipo consideren que es fundamental para la organización. Una vez que se complete el análisis del activo, el equipo puede ampliar la evaluación para otros activos críticos.

El líder a menudo reúne el equipo de análisis después de obtener el patrocinio de alto nivel de gestión para la evaluación. El Jefe del departamento de TI sería un buen candidato para ser el líder del proyecto.

OCTAVE-S no es una evaluación de vulnerabilidad típica que se centra exclusivamente en cuestiones tecnológicas. Porque también se ocupa de los negocios, OCTAVE-S es una evaluación del riesgo operacional que es similar al proceso de negocio o de gestión de las evaluaciones tradicionales. Es útil si alguien en el equipo de análisis está familiarizado o ha realizado evaluaciones y toma de decisiones. Al menos un miembro del equipo de análisis debe tener cierta familiaridad con la infraestructura

informática de la organización o debe ser el punto de contacto con los proveedores que configuran y mantienen la infraestructura de computación. La persona que tiene familiaridad con la infraestructura tiene que entender los procesos básicos de seguridad de la información de la organización.

3. Ajuste del alcance apropiado del método OCTAVE. La evaluación debe incluir importantes áreas operativas, pero el alcance no puede ser demasiado grande. Si es demasiado amplio, será difícil para el equipo de análisis analizar toda la información. Si el alcance de la evaluación es demasiado pequeño, los resultados pueden no ser tan significativos como deberían ser.

   Se seleccionará las áreas operacionales que reflejen las funciones principales operativas o comerciales, así como las funciones importantes de apoyo de la organización. Las áreas operativas seleccionadas para la evaluación deben representar las más críticas para el éxito de la organización o las que tienen el riesgo más alto.

   • Al menos cuatro áreas son recomendadas, una tiene que ser el departamento de TI.
   • Hay que tener en cuenta el compromiso de tiempo que necesite el personal y si habrá conflictos significativos con las operaciones en curso.
   • Considerar las áreas que requieren de información electrónica para llevar a cabo sus funciones.
   • Considerar las áreas en las que los sistemas e información electrónica estén más expuestos al riesgo.
   • Considerar las áreas críticas que afectarían las operaciones de la organización si estas fallaran.

   Se deberá registrar los nombres de las áreas operacionales seleccionadas en la hoja de trabajo. Si se ha seleccionado el equipo de análisis antes de establecer el alcance de la evaluación, se deberá asegurar de que los

miembros del equipo tienen comprensión de las áreas operativas que se evalúan. Si el equipo no tiene suficiente conocimiento de una o más áreas, es posible que necesite ajustar la composición del equipo.

Cómo selección de las áreas claves operativas en CNEL se tienen: el área de planificación, financiera, comercial, técnica, jurídica, gestión de riesgo y talento humano que son críticas para que la empresa logre su misión.

En este punto, se debe estar preparado para planificar cómo se va a realizar la evaluación.

4. La selección de los participantes. Durante los talleres de recolección del conocimiento (procesos 1 a 3), los miembros del personal de varios niveles de organización aportarán sus conocimientos sobre la organización. Ellos deben ser asignados a los talleres debido a sus conocimientos y habilidades, no sólo en función de quién está disponible.

   Los miembros de las áreas relacionadas con el negocio deben tener una amplia visión de cómo se utilizan los sistemas e información para apoyar los procesos y / o el conocimiento del negocio de la organización en las políticas. Se pueden incluir hasta 3 miembros del equipo de análisis de las unidades relacionadas con el negocio.

   Se escogerá a personas que tengan una amplia visión de cómo los sistemas y la información son utilizados para apoyar los procesos de negocio de la organización. Además, deberán tener idea clara de las políticas y procesos. Para esto se seleccionarán personas del departamento de Planificación y Gestión de Riesgo.

   Se seleccionará al Jefe del departamento de TI y un ingeniero informático para el equipo de análisis ya que estos tienen conocimiento de la infraestructura informática, el funcionamiento y configuración de los sistemas, redes, y su mantenimiento.

Una vez que los miembros del equipo de análisis hayan sido seleccionados, al menos un miembro del equipo necesita familiarizarse con OCTAVE-S. Lo ideal sería que todos los miembros del equipo lleguen a conocer la metodología. Sin embargo, las limitaciones de organización (por ejemplo, los fondos disponibles, el tamaño de la organización) pueden limitar el número de personas que pueden invertir el tiempo para familiarizarse con el proceso.

Los miembros del equipo que tienen la tarea de aprender acerca de OCTAVE-S pueden participar en la formación formal o familiarizarse con el proceso por su cuenta. (Por ejemplo, a través de la guía de implementación de OCTAVE).

El objetivo de la preparación es asegurarse de que la evaluación tenga un alcance correcto, que los altos directivos de la organización aprueben y apoyen el proceso, y que todos los participantes comprendan su función.

Una vez que se ha completado la preparación para el método de OCTAVE, la organización está lista para comenzar la evaluación. A partir de este punto, se puede hacer uso de la guía de implementación de las fases de OCTAVE en el sitio web de CERT, junto a las hojas de trabajo y otros recursos.

El método OCTAVE involucra dos tipos de talleres: (1) conversaciones con varios miembros de la organización y (2) talleres en los que el equipo de análisis lleva a cabo una serie de actividades por cuenta propia. Todos los talleres tienen un líder y un escribiente.

El líder es responsable de guiar todas las actividades del taller y asegurar que todas ellas (incluyendo las actividades preparatorias y de seguimiento) se hayan completado. El líder también es responsable de asegurar que todos los participantes comprendan sus funciones y que todos los miembros nuevos o complementarios del equipo de análisis estén dispuestos a participar activamente en el taller. Todos los líderes de los talleres también deben asegurarse de que se seleccionen un método de toma de decisiones (por ejemplo, el voto mayoritario, el consenso) que se utilizará durante los talleres.

Los escribas son responsables de registrar la información generada durante los talleres, ya sea electrónicamente o en papel. Se debe tener en cuenta que puede que no se tenga el mismo líder o escriba para todos los talleres. Por ejemplo, un líder con más facilitación o habilidades para la entrevista puede ser adecuado para los talleres de la fase 1, mientras que un líder con gran capacidad de planificación y análisis podría ser preferible para los talleres de la fase 3.

6.5.1. Metas del proceso OCTAVE-S

En la fase 1, se conoce a la organización, sus prácticas y activos; los activos pueden ser la información, hardware, sistemas o personas.

En la fase 2, hasta 5 de los activos relacionados a la información de la organización han sido designados como críticos y se ha documentado por qué se los ha elegido.

Se han creado perfiles de amenazas para cada activo, cada perfil contiene: un conjunto de árboles de amenazas, ejemplos específicos de amenazas humanas, la fuerza del motivo si aplica y el nivel de confianza asociada, la historia de cada amenaza.

En la fase 3, se tiene un entendimiento amplio de cómo se usa la tecnología de la información, y el ambiente de negocio. Se identifican los sistemas para cada activo, puntos de acceso de red, administradores, y se examina la resistencia a ataques.

En la fase 4, se identifica y analiza riesgos basandose en el impacto, la historia y la probabilidad tomando valores cuantitativos como alto bajo y medio.

En la fase 5, se planifican las estrategias de mitigación contra las amenzas encontradas.

6.5.2. Cronograma

OCTAVE-S se lleva a cabo mediante una serie de reuniones; el horario para la realización de estas reuniones es bastante flexible. El marco de tiempo más breve posible para completar una evaluación en su conjunto es de aproximadamente dos días. Esta estimación asume un tiempo completo, con un equipo de análisis dedicado que tiene experiencia con el proceso y una evaluación cuyo ámbito es estrecho (por ejemplo, para una o dos áreas operativas). Las limitaciones prácticas pueden extender el tiempo requerido para llevar a cabo OCTAVE-S. Al programar las actividades de evaluación, se debe:

- Considerar las limitaciones de la organización.
- Asignar tiempo suficiente para completar todas las actividades de preparación.
- Recordar que todos los planes son estimaciones.
- Revisar el plan del proyecto para reflejar los cambios apropiados.

A continuación, se menciona un estimado de las actividades más importantes en el proceso OCTAVE-S para CNEL, los tiempos están basados según la guía OCTAVE de preparación (2005) para un equipo sin experiencia previa como sería el actual caso.

Implementación OCTAVE	**TIEMPO ESTIMADO**	**ENCARGADO**
Etapa de Preparación		
Obtener apoyo de la administración para OCTAVE-S	1 semana	Líder del proyecto
Seleccionar y entrenar al equipo de análisis	1 semana	Líder del proyecto
Establecer el alcance de la evaluación	1 día	Equipo de análisis
Planificar la ejecución OCTAVE-S	4 horas	Encargado de la logística
Preparar cada proceso OCTAVE-S	4 horas / proceso (fase)	Equipo de análisis
Fase 1		
Identificar información organizacional		Equipo de análisis
Establecer el impacto de los criterios de evaluación	3 horas	Equipo de análisis
Identificar activos organizacionales	3 horas	Equipo de análisis
Evaluar prácticas de seguridad organizacionales	6 horas	Equipo de análisis
Fase 2		
Crear perfiles de amenazas		Equipo de análisis
Seleccionar activos críticos	2 horas	Equipo de análisis
Identificar requerimientos de seguridad	6 horas	Equipo de análisis
Identificar amenazas a los activos críticos	12 horas	Equipo de análisis
Fase 3		
Examinar la infraestructura en relación a los activos		
Examinar rutas de acceso	4 horas	Equipo de análisis
Analizar los procesos relacionados a la tecnología	4 horas	Equipo de análisis
Fase 4		
Identificar y analizar los riesgos		
Evaluar el impacto de las amenazas	10 horas	Equipo de análisis
Establecer criterios basados en la frecuencia	8 horas	Equipo de análisis
Fase 5		
Desarrollar estrategias y planes de mitigación		
Describir la estrategia de protección actual	4 horas	Equipo de análisis
Desarrollar un plan de mitigación	8 horas	Equipo de análisis
Identificar cambios a la estrategia de protección	6 horas	Equipo de análisis

Fig.3 Cronograma de implementación de OCTAVE-S

6.6. Conclusiones

- Se observa que la Unidad de Negocio de la empresa estudiada tiene poco conocimiento del tema de gobierno de Tecnologías de la Información (TI), por este motivo le faltan herramientas, para demostrar con resultados, que involucrar las tecnologías a la alta gerencia trae para la organización un retorno positivo.

- OCTAVE es una herramienta que incrementará la conciencia de iniciativas de seguridad y ayudará a los gerentes a entender riesgos fuera de sus áreas.

- La metodología seleccionada permite que se adapte a características propias de la organización, la infraestructura, operaciones, el nivel de experticia de los usuarios, para garantizar que los procedimientos seleccionados cumplan con el cometido de garantizar la salvaguarda adecuada de todos los datos e información.

- La propuesta de intervención permite complementar los procesos externos de auditoría para la Unidad de Negocio, además de contribuir con las regulaciones gubernamentales para empresas públicas y estándares de calidad de seguridad informática como la ISO 27001.

7. Referencias Bibliográficas

Alfafara (2011). Overview of Frameworks: Cobit, COSO, Recuperado de: https://www.resourcenter.net/images/AHIA/Files/2009/AnnMtg/Handouts/C3.pdf

Aucancela (2002). AUDITORIA DE RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE SISTEMAS DE CAVES SA EMA UTILIZANDO COBIT COMO MARCO DE REFERENCIA [En línea] Recuperado de: repositorio.espe.edu.ec/bitstream/21000/6095/1/T-ESPE-034400.pdf [Accedido el 24 Ene. 2016].

CERT (2005). Home. [En línea] Recuperado de: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795 [Accedido el 24 Ene. 2016].

Contraloría General del Estado Ecuatoriano, (2009). NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS. [En línea] Recuperado de: http://www.contraloria.gob.ec/normatividad_vigente.asp [Accedido el 18 nov. 2015].

Conza & Medrano (2002). Análisis de riesgos informáticos y elaboración de un plan de continuidad para la unidad de educación virtual CEC-EPN [En línea] Recuperado de: http://dspace.udla.edu.ec/bitstream/33000/4473/1/UDLA-EC-TIS-2015-02.pdf [Accedido el 24 Ene. 2016].

COSO (2016). Home. [En línea] Recuperado de: http://www.coso.org/ [Accedido el 24 Ene. 2016].

Cuellar (2013). Teoría General de la Auditoría y Revisoría Fiscal. [En línea] Recuperado de: http://fccea.unicauca.edu.co/old/tgarf/tgarfse88.html [Accedido el 24 Ene. 2016].

Dean (2002). La investigación tecnológica en las ciencias de la ingeniería y la innovación tecnológica. [En línea] Recuperado de: http://www.unrc.edu.ar/publicar/23/dossidos.html [Accedido el 24 Ene. 2016].

Explorable (Nov 3, 2009). Investigación Cuantitativa y Cualitativa. Ene 21, 2016 Recuperado de: https://explorable.com/es/investigacion-cuantitativa-y-cualitativa.

Gaona (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala [En línea] Recuperado de: http://dspace.ups.edu.ec/handle/123456789/5272 [Accedido el 24 Ene. 2016].

Gallardo & Jácome, (2011). Análisis de riesgos informáticos y elaboración de un plan de contingencia TI para la Empresa Eléctrica Quito S.A [en línea] Recuperado de: http://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf/ [Accedido el 24 Ene. 2016].

Granda, (2011). Diseño de un plan de contingencias de tics para la empresa eléctrica Centrosur [en línea] Recuperado de: http://dspace.ucuenca.edu.ec/bitstream/123456789/2556/1/tm4534.pdf [Accedido el 24 Ene. 2016].

ISO/IEC, (2005). ISO/IEC 27001:2005 Information technology – Security techniques -- Specification for an Information Security Management System. Geneva, Switzerland: ISO/IEC.

ISACA, (2006). CISA Review Manual 2006. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3.

Jara, (2011). Políticas de seguridad de la información aplicadas a una red local de cybercafé [online] Recuperado de: http://dspace.uazuay.edu.ec/bitstream/datos/2495/1/08361.pdf [Accedido el 24 Ene. 2016].

Jiménez (2008). ¿Por qué necesitamos el Análisis de Riesgo en T.I.? [en línea]. Recuperado de:http://ci.ucr.ac.cr/sites/default/files/informaciondigital/por_qu%C3%A9__analisis_de_riesgo_en_ti__%28art35a-ci%29_v1-0.pdf [Accedido el 24 Ene. 2016].

Kiran, K., Reddy L., Lakshmi L., (2013). A comparative risk assessment Information Security Models. *International Journal of Computer Applications.* p.2

Ministerio del Interior, (2014). Normas técnicas de control interno. [online] Recuperado de:http://www.ministeriointerior.gob.ec/wpcontent/uploads/downloads/2014/03/NORMAS-TECNICAS-DE-CONTROL-INTERNO.pdf/ [Accedido el 24 Ene. 2016].

Moncayo, (2014). Modelo de evaluación de riesgos en activos de TIC'S para pequeñas y medianas empresas del sector automotriz [online] Recuperado de: http://bibdigital.epn.edu.ec/handle/15000/8499 [Accedido el 24 Ene. 2016].

National Technical Authority for Information Assurance, (CESG), (2015). Managing information risk - Detailed guidance - GOV.UK. [en línea] Recuperado de: https://www.gov.uk/guidance/managing-information-risk [Accedido el 18 Nov. 2015].

National Technical Authority for Information Assurance, (CESG), (2015). Analysis of information risk management methodologies. [en línea] Recuperado de: https://www.gov.uk/guidance/analysis-of-information-risk-management-methodologies [Accedido el 18 nov. 2015].

Páez, (2013). APLICACIÓN DE LA NORMA OCTAVE-S EN LA EMPRESA PIRÁMIDE DIGITAL CIA. LTDA [en línea] Recuperado de: http://repositorio.puce.edu.ec/bitstream/handle/22000/6226/T-PUCE-6401.pdf?sequence=1&isAllowed=y [Accedido el 24 Ene. 2016].

Padilla (2012). Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua (Tesis de pregrado). Universidad Técnica de Ambato. Ecuador.

Paredes & Vega (2011). Desarrollo de una metodología para la auditoría de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura (Tesis de pregrado). Universidad Técnica de Ambato. Ecuador.

Reyes (2014). “El análisis de riesgos informáticos y su incidencia en la seguridad e integridad de la información en la facultad de ingeniería civil y mecánica de la Universidad Técnica de Ambato.” [En línea] Recuperado de: http://repo.uta.edu.ec/bitstream/123456789/6987/1/Tesis_t871mif.pdf [Accedido el 24 Ene. 2016].

Sangoluisa (2015). Definición de las políticas de seguridad de la información para convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000 [En línea] Recuperado de: http://bibdigital.epn.edu.ec/handle/15000/11462 [Accedido el 24 Ene. 2016].

Tinoco, Aguirre, Merchán (2012). Guía de Auditoría para la Evaluación del Control Interno de TI en las Entidades Públicas, [en línea] Recuperado de: http://repositorio.espe.edu.ec/bitstream/21000/8382/1/AC-EAST-ESPE-047888.pdf [Accedido el 18 nov. 2015].

Tomhave (2006). The Total Enterprise Assurance Management (TEAM) Model: A Unified Approach to Information Assurance Management [en línea] Recuperado de: http://www.secureconsulting.net/Papers/Tomhave_Thesis-FINAL.pdf [Accedido el 18 Nov. 2015].

8. Anexos

ANEXO 1

Normativa de Control Interno del Ecuador

A fin de realizar el análisis de las metodologías para garantizar una buena gestión, se revisó la Evaluación de Control Interno de la Norma 410 – Tecnología de la Información, que forma parte de las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que disponen de Recursos Públicos, que fueron emitidas por la Contraloría General del Estado tal como lo señala la Ley Orgánica de Empresas Públicas.

Estas normativas engloban las siguientes secciones resumidas por Tinoco, Aguirre y Merchán (2012).

Organización y administración

- Estructura Organizacional
  - Organigrama de la Unidad de Tecnología de Información y Comunicación.
  - Orgánico funcional aprobado.
- Segregación de Funciones
  - Descripción documentada y aprobada de los puestos de trabajo.
  - Resultados de la evaluación de desempeño.
- Plan Informático Estratégico y Tecnología
  - El Plan estratégico y operativo de tecnología de información y su presupuesto analizados y aprobados por la máxima autoridad de la entidad y que al menos incluya: o Políticas y Procedimientos.
  - Políticas y procedimientos aprobados por la máxima autoridad y difundidos

- Modelo de Información Organizacional
    - Diccionario de datos, Modelo entidad – relación, Modelo físico.
- Proyectos Tecnológicos
    - Documentos entregables con sus respectivas aprobaciones, documentos formales como actas o documentos electrónicos legalizados.
    - Plan de control de cambios aprobado
    - Plan de aseguramiento de la calidad aprobado o Capacitación.
    - Plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.
- Comité Informático.
    - Resolución de la entidad en donde se encuentre: creación y objetivos, integración, funciones, sesiones, subcomisiones de apoyo

Sistemas Informáticos

- Políticas de Software
- Políticas y estándares de software aprobados y difundidos.
- Metodologías y procedimientos definidos en el desarrollo de software.

Adquisición de Software

- Plan Anual de Compras de la Institución, Portafolio de proyectos, Documento que se solicita el requerimiento, la necesidad, Pliegos, Contrato, Actas entrega-recepción.
- Procedimiento precontractual, contractual y ejecución que se realiza en el Sistema Nacional de Compras Públicas.

Desarrollo de Software

- Portafolio de proyectos y servicios.
- Requerimientos funcionales y técnicos Actas de aceptación por parte de los usuarios.

- Manuales técnicos, instalación, configuración, y de usuario o Mantenimiento de Software.
- Procedimientos para el mantenimiento y liberación del software de aplicación.
- Registro del control de cambios.
- Registro de control de versiones.
- Manuales técnicos y de usuarios actualizados.
- Verificar si existe ambientes de desarrollo, prueba y producción.
- Diagramas y configuraciones de hardware y software o Aplicaciones y Servicios
- Instructivos de instalación, configuración y uso de los servicios de intranet, internet y correo electrónico.

Infraestructura Tecnológica

- Administración de la Infraestructura o Adquisición de Infraestructura
- Plan Anual de Compras de la Institución, Portafolio de proyectos, Documento que se solicita el requerimiento, la necesidad, Pliegos, Contrato, Actas entrega-recepción.
- Los mismos procedimientos precontractuales y contractuales aplicados por el Sistema Nacional de Compras Públicas.
- Determinar la correspondencia de las características técnicas entre los equipos adquiridos, especificaciones técnicas y requerimientos establecidos en las fases precontractual, contractual y confirmado en las actas entregas recepción.

Mantenimiento y Soporte de la Infraestructura

- Políticas y procedimientos emitidos para el mantenimiento de la infraestructura tecnológica.
- Plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica.

Seguridades

- Políticas y procedimientos aprobados y difundidos para proteger y salvaguardar los bienes y la información.
- Constatación física de la ubicación e instalaciones físicas de la Unidad de Tecnología de Información y del Centro de Datos.
- Políticas y procedimientos para la obtención de respaldos.
- Plan de Contingencia aprobado e implementado

Monitoreo y Evaluación

- Procesos y Servicios
- Indicadores de desempeño definidos
- Medidas o procedimientos definidos para el análisis de satisfacción al cliente
- Informes de gestión
- Metodologías utilizadas para la evaluación y monitoreo

ANEXO 2

Entrevista a funcionarios de CNEL Esmeraldas

1. **¿Cuántas personas laboran en la institución? ¿Cómo se encarga de la gestión de riesgos en la empresa? ¿Cuantas personas hay en el departamento de TI?**

   Existen 400 empleados en total (administrativos y obreros) de los cuales 120 son funcionarios administrativos. La empresa se constituye en forma de corporación en la cual la Oficina Central se encuentra en Guayaquil, la segregación de funciones de TI se divide en Jefe de Sistemas, Programador, Soporte Técnico, Comunicaciones y Servidores. Existe un departamento de gestión de riesgo ocupacional en la empresa que se encarga de riesgos ambientales. Se les ha indicado que se haga una gestión de activos para darlos de baja cuando estén dañados y enviarlos a una unidad ambiental.

2. **¿Tiene una organización con estructura tradicional o adaptativa?**
   Tenemos una estructura organizacional adaptativa.

3. **¿Cómo se maneja la seguridad de la información en la Unidad de Negocios Esmeraldas?**

   La Oficina Central se le ha proporcionado a la Unidad procedimientos sobre como respaldar información, solicitar información, procesos de garantía.

   Todas las máquinas están dentro de un directorio activo (políticas) por cada Unidad de Negocio, servidor de Antivirus, servidor de Firewall son los controles de seguridad que maneja la Unidad.

   En Oficina Central (Guayaquil) se alojan las aplicaciones en el datacenter y otras aplicaciones locales que se replican allá. El Director de Tecnología y Gerente de tecnología manejan las áreas de Aplicaciones, Redes, Seguridad. Dependiendo del

área hay procesos o viene el personal hasta Esmeraldas hacen un muestreo y hacen un diagnóstico.

4. **En cuanto a la filosofía de la seguridad: CIA ¿Tiene algún énfasis?**

Depende, el servidor de GIS es local, solo accede el administrador de Esmeraldas y el administrador del centro de datos puede monitorear, pero no tiene acceso a los datos, estos se replican en la administración central, y se hacen respaldos continuamente sobre la administración de Esmeraldas y Oficina Central.

Se tiene un servidor en el que se almacena sistemas. Un sistema desarrollado para el servidor cada noche hace un respaldo. Si hay un siniestro ocurre se cuenta con un respaldo.

Se tiene procesos definidos para el manejo de información y respaldo en el documento de políticas de la Corporación.

5. **¿Le gustaría tener software que automatice el proceso, que se ayude de una base de conocimiento o le gustaría tener un analista de riesgos?**

Se usa mucho el software libre y procuramos usar herramientas open source para evitar costos.

No se usa ninguna metodología y los procesos de evaluación se hacen de una forma general, no minuciosa. Se desea aplicar una metodología.

6. **¿Necesita que la administración sea consultada para poder implantar una metodología para la gestión de seguridad informática ¿Es de importancia estratégica?**

Se tiene tiempo que se puede planificar, personal, pero no los recursos ya que cualquier requerimiento se necesita pedir a la Oficina Central lo que incurre en mucha burocracia.

Le gustaría un personal que determine y evalúe los riesgos. Pero el problema la oficina, que deben tener una aprobación. que van a ganar, que va a ganar la organización.

No se conoce si existe una herramienta para la evaluación de riesgos en la oficina central.

7. **¿Requiere argumentos simples o argumentos complejos en el reporte de un análisis de riesgos?**

   Se requiere argumentos simples pero concisos para poder mitigar los riesgos fácilmente, además no se encuentra incidencias de riesgos frecuentemente como para llevar argumentos más complejos.

8. **¿Tiene los recursos suficientes para emplear más de una metodología? ¿O le gustaría emplear solo una?**

   La asignación de recursos es manejada por la Oficina Central de la Corporación, se tiene la política de asignar recursos sólo para fines factibles y que van a ayudar a la Unidad y a la Corporación en general, invertir en más de una metodología puede verse como un desperdicio de los recursos.

9. **¿Desea contratar expertos en seguridad que se especialicen en un método particular? ¿Desea entrenar a sus propios analistas para el uso de un método?**

   Les gustaría contratar una persona que sepa de gestión de riesgos informáticos.

10. **¿Cuál es el nivel de riesgos de sus procesos (s)?**

    Es relativamente bajo.

11. **¿Necesita una metodología que siga todos los pasos en la evaluación de riesgos? (identificación de riesgos, análisis de riesgos, gestión de riesgos y procedimientos de monitoreo)**

    Si.

12. ¿Cree que la administración implementara las recomendaciones dadas por el método seleccionada?

Si pueden mitigar riesgos importantes encontrados, sí.

13. ¿Estaría dispuesto a invertir tiempo en la cuantificación de perdida financiera?

No, ya que estos tipos de análisis no se encuentran actualmente en la competencia de la Unidad de Negocios y son generalmente manejados por la Oficina Central de la Corporación. Esto implica que un enfoque cualitativo es lo más idóneo en la Unidad.

14. ¿Qué herramientas usa la empresa para la evaluación de riesgos?

Se hace una auditoría anual con la ayuda de un software llamado OCS Inventory, este es un software gratis que permite hacer un inventario de activos, referente a la estructura, equipos y otros activos.

15. ¿Si está usando un framework para la gestión de riesgos, por qué lo usó? ¿Su industria influyó en la elección? (ITIL, ISO, etc.)

Se desconoce en la Unidad, pero se sabe que la normativa de Control Interno de la Contraloría está basada en marco de control COSO.

16. ¿Cuál es el alcance que le gustaría tener en una metodología de gestión de riesgos? ¿Qué activos le preocupan?

Se desarrollan sistemas locales pequeños e interfaces, una aplicación comercial donde se tiene una pequeña base de datos local y el usuario necesita ejecutar procesos rápidos con los cuales se usa la interface que es una app que interactúa con una base de datos y otro programa. Y con los programas locales para agilitar procesos internos.

17. ¿Cuáles son los mayores riesgos de la compañía, que tan severo es su impacto y que tan probable es que ocurran?

El riesgo más grande es la perdida de la información. Se perdió la información del disco donde se tenía los respaldos hace 3 años. En el momento en que ocurrió se tenía respaldo no actualizado. Ya no se maneja información como antes y ahora esa información se maneja en la oficina central.

18. ¿Cómo se da el proceso de auditoria informática?

CNEL tiene un proceso de auditoría externa. Todos los años al termino del año fiscal, auditoria revisa todo lo que se ha trabajado. La auditoría se hace en todas las áreas de la empresa. El área de sistemas tiene un auditor especializado, que pide información sobre los procesos, estructura organizacional, funciones, y proceso de respaldo. Al fin de la auditoria, se hace un informe acerca de la seguridad de la información.

En el caso de que no se estén siguiendo los procesos adecuadamente, el auditor genera un informe técnico al Administrador de la Unidad de Negocio con las indicaciones.

La auditoría se hace a todos los departamentos por la Contraloría General del Estado por 3 semanas. Sus observaciones fueron sobre el centro de datos y mejorar los racks, esto está presupuestado para el año 2017.

Hasta la fecha no ha habido penalizaciones por irregularidades en las auditorías de la Controlaría.