PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN SISTEMAS

"APLICACIÓN DE LA NORMA OCTAVE-S EN LA EMPRESA PIRÁMIDE DIGITAL CIA. LTDA"

OLGA PÁEZ OBANDO

DIRECTOR: ING. JAIME NARANJO

QUITO, 2013

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de disertación tiene como objetivo aplicar la norma OCTAVE-S en la empresa Pirámide Digital Cía. Ltda., para realizar una evaluación de amenazas críticas, activos y vulnerabilidades que propone OCTAVE-S (Operationally Critical Threat, Asset and Vulnerability Evaluation) mediante un enfoque en el que se define una evaluación estratégica basada en el riesgo.

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

OCTAVE-S es una variación del enfoque adaptado a restricciones y limitaciones únicas que se encuentran típicamente en pequeñas y medianas organizaciones.

OCTAVE-S está dirigida por un pequeño equipo interdisciplinario del personal de la organización que se reúne y analiza información, producen una estrategia de protección y planes de mitigación basados exclusivamente en los riesgos de seguridad de la organización

Para llevar a cabo OCTAVE-S efectivamente, el equipo debe tener un amplio conocimiento de lo que realiza la organización y los procesos de seguridad con los que cuenta la empresa.

Se seleccionó la empresa Pirámide Digital debido a que tuve acceso a la información y apertura para trabajar con las personas que trabajan ahí, además es una empresa pequeña y desde el día que se propuso trabajar con ellos me abrieron las puertas a su organización.

DEDICATORIA

Quiero agradecer a Dios por haberme dado la fuerza para continuar y terminar mi carrera en los momentos en los que más necesitaba aliento.

A mis padres por haberme apoyado desde el primer día que entré a la universidad, especialmente a mi mamá por siempre haber estado pendiente de mí, alentándome, porque siempre ha confiado en mí y en lo que puedo hacer, por sus consejos y sus valores, su motivación que me ha convertido en la persona que soy, pero más que nada por su amor. A mi papá por sus ejemplos de constancia y perseverancia que lo caracterizan, los que me ha influido siempre.

A mi tío Ferdi y mi tía Olgui, porque desde el primer día han sido como mis segundos padres y siempre, cuando más los he necesitado han estado para mí, apoyándome incondicionalmente, estaré eternamente agradecida de tenerlos en mi vida.

A mi abuelita Luky, de quien he aprendido a ser más fuerte, gracias por enseñarme a ser una mujer valiente, por tu cariño y todo lo que me has dado.

A mi tía Dini, quien con su cariño incondicional ha estado siempre pendiente de mí, gracias por su presencia, su dulzura y por siempre confiar en mí.

A mi hermana Anita por ser mi amiga, nunca has dejado de estar a mi lado; admiro tu coraje, fortaleza y empeño.

To Nick, for always being there for me, supporting me and making me believe the sky is the limit I love you to the moon and back.

Y por último a Melcocha, por su fidelidad, por estar a mi lado y ser una amiga incondicional.

AGRADECIMIENTO

Quiero expresar mi sincero agradecimiento al Ing. Jaime Naranjo por guiarme en el trabajo de esta Tesis, por sus enseñanzas, por compartir conmigo su conocimiento y experiencia, por el valor agregado que aporta a este trabajo de disertación. Gracias por su apoyo.

A mis correctores Ing. Beatriz Campos por ser más que mi profesora una guía a lo largo de toda mi carrera. Ing. Alfredo Calderón gracias por sus conocimientos, paciencia, experiencia y el tiempo que dedicó para trabajar conmigo.

A mis amigos por haberme apoyado a lo largo de mis años universitarios.

RESUMEN EJECUTIVO

Esta Tesis tiene como Objetivo General aplicar la norma Octave-S en la empresa Pirámide Digital para realizar una evaluación del manejo de riesgos en seguridad informática.

El Capítulo Uno sirve como marco teórico en donde se menciona y explican conceptos generales sobre análisis de riesgos, análisis de seguridades y cómo el enfoque OCTAVE utiliza una valoración de evaluación de riesgos basada en los activos a más de un cuadro comparativo entre OCTAVE-S, ISO 1779 y COBIT 4.1 y se justifica con esta tabla por qué se seleccionó a OCTAVE-S para realizar el análisis de riesgos en la empresa.

En el Capítulo Dos se justifica el uso de COBIT 4.1 para evaluar la situación actual de la empresa en base al cuadro comparativo presentado en el Capítulo Uno, se describe la caracterización de la empresa y a través de matrices de madurez se evalúan los cuatro dominios que propone COBIT 4.1: planeación y organización, adquisición e implementación, entrega y soporte y monitoreo y evaluación; para esto se escogieron once procesos:

- PO1: Definir el plan estratégico de TI
- PO3: Determinar la dirección tecnológica
- PO4: Definir procesos, organización y relaciones de TI
- PO9: Evaluar y administrar riesgos de TI
- AI5: Instalar y acreditar sistemas
- AI6: Administrar cambios
- DS1: Definir y administrar niveles de servicio
- DS5: Garantizar la seguridad de los sistemas
- DS10: Administrar los datos

- ME1: Monitorear el desempeño de TI
- ME2: Monitorear y evaluar el control interno

En el Capítulo Tres se aplica la norma OCTAVE-S antes de iniciar la evaluación, se describen los roles, responsabilidades y habilidades del equipo de trabajo, se indica el perfil de los altos directivos, directivos de áreas operativas y del personal en general para que se pueda seleccionar al equipo de trabajo que colaborará en la evaluación.

Una vez que se seleccionó al equipo de trabajo, se inició la evaluación utilizando la metodología que propone OCTAVE-S la cual se divide en tres fases; en la Fase Uno se construye un perfil de amenaza basado en los activos de la empresa, esta fase cuenta con los siguientes procesos: identificar la información organizacional y 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 practicas organizacionales, seleccionar activos críticos, identificar requerimientos de seguridad e identificar amenazas a los activos críticos.

La Fase Dos sirve para identificar vulnerabilidades de la infraestructura y cuenta con un solo proceso en el que se examina la infraestructura computacional en relación a los activos críticos para lo que se definen las siguientes actividades: examinar rutas de acceso y analizar los procesos relacionados con tecnología.

Finalmente, 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 para lo que 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.

En el Capítulo Cuatro, se presenta un informe preliminar y un informe ejecutivo dirigidos y validados por el Gerente General de la empresa Pirámide Digital Cía. Ltda.

Finalmente en el Capítulo Cinco se presentan las conclusiones y recomendaciones a las que se han llegado una vez concluido el proyecto de titulación realizado.

CAPITULO UNO

1.1 Análisis de Riesgos

Los diferentes casos relacionados con la necesidad de mejorar la seguridad de la información de las empresas aumentan diariamente; las amenazas siempre han existido, la única diferencia es que actualmente, estas amenazas son mucho más difíciles de detectar y mucho, más rápidas. Por estas razones, las empresas deben estar siempre en alerta y conocer qué sistemas de seguridad puede implementar, realizando previamente un análisis de riesgos que permita evitar o minimizar las consecuencias no deseadas y no esperadas. Es importante tener en cuenta que previamente a implementar un sistema de seguridad, se debe conocer de forma detallada el entorno de los procesos de negocio de la organización, lo que permitirá priorizar las acciones de seguridad que se deben aplicar a los procesos clave del negocio, los más críticos y los que están vinculados a cumplir los objetivos de la organización.

El análisis permite rastrear las distintas amenazas que pueden afectar a activos vulnerables y permite que se generen recomendaciones las que hacen más sencilla la corrección de los activos y qué se debe hacer para protegerlos, este análisis tiene como fin detectar los riesgos de los cuales los activos pueden ser víctimas y que probabilidad de ocurrencia existe. Toda amenaza se puede convertir en realidad, es por ello que el momento que se la detecte debe ser eliminada al máximo para que el ambiente que se busaca proteger se encuentre libre de riesgos de incidentes de seguridad.

El análisis de riesgos, se define como:

Una actividad centrada en la identificación de fallas de seguridad que evidencien vulnerabilidades que pueden ser explotadas por amenazas, provocando impactos en los negocios de la organización: es una actividad de análisis que pretende, a través del rastreo, identificar los riesgos a los cuales los activos se encuentran expuestos. [1]

[1] Lozano, Javier. Seguridad de la Información. Riesgos. Internet. www.elmayorportaldegerencia.com/ documentos/188-tecnologias-de-informacion-y-comunicación Acceso: (27 de diciembre de 2012)

Además, es una actividad que busca encontrar la consolidación de las vulnerabilidades que permitan identificar los pasos que se deben seguir para su corrección, identificar las amenazas que pueden explotar las vulnerabilidades para corregirlas o eliminarlas, identificar los impactos potenciales que pudieran tener los incidentes, aprovechar las vulnerabilidades encontradas y determinar las recomendaciones para que las amenazas sean corregidas o reducidas.

El análisis de riesgos como el primer elemento de la acción de seguridad, es un factor determinante para los distintos procesos críticos en los que se analizan todas las amenazas de las que pueden ser víctimas. De esta manera, son considerados y analizados todos los activos de la organización, para que estén libres de vulnerabilidades, con el propósito de reducir los riesgos.

"Un análisis de riesgos tradicional se construye por medio de un conjunto de actividades preestablecidas que tiene como objetivo: identificar el proceso a considerar, saber cuáles son sus elementos o partes constituyente y cuáles son los equipos necesarios para efectuarlo.[2]"

El primer paso para realizar un análisis de riesgos es identificar la relevancia de cada uno de los procesos de la empresa, para priorizar las acciones de seguridad e iniciar el trabajo de implementación de seguridad en las áreas estratégicas que puedan generar un mayor impacto en la organización, si se llegara a presentar un incidente.

El segundo paso, es determinar la relevancia de los activos determinantes para el proceso del negocio, lo cual marca un rumbo definitivo de las acciones de seguridad en la empresa, se debe asegurar que los activos cumplan con su propósito, en cuanto a la seguridad de la información y garantizar su confidencialidad, integridad y disponibilidad.

El análisis de seguridad es el reconocimiento de todo el entorno en el que se pretende implementar normas de seguridad para que puedan cumplir los siguientes propósitos:

[2] Lozano, Javier. Seguridad de la Información. Riesgos. Internet. www.elmayorportaldegerencia.com/ documentos/188-tecnologias-de-informacion-y-comunicación Acceso: (27 de diciembre de 2012)

- Identificar los puntos débiles, para que sean corregidos y así disminuir las vulnerabilidades presentes en los activos de los procesos de negocios.
- Conocer los elementos constituyentes de la infraestructura de comunicación, procesamiento y almacenamiento de la información, para dimensionar dónde serán hechos los análisis y cuáles elementos serán considerados.
- Conocer el contenido de la información manipulada por los activos, con base en los principios de la confidencialidad, integridad y disponibilidad.
- Dirigir acciones para incrementar los factores tecnológicos y humanos en las áreas críticas y desprotegidas.
- Permitir una gestión periódica de seguridad, con el objetivo de identificar nuevas amenazas y vulnerabilidades, además de la verificación de la eficacia de las recomendaciones provistas[3]

El enfoque Octave define al análisis de riesgos como:

Un análisis efectivo que considera tanto los aspectos organizativos y tecnológicos, examinando cómo la gente usa la infraestructura informática de su organización en una base diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora de la seguridad, ya que genera una vista de toda la organización de los riesgos de seguridad de la información, proporcionando una base para la mejora.[4]

Hay muchas normas, prácticas y métodos disponibles para hacer frente a los riesgos de seguridad de la información. Seleccionar la opción correcta de una organización, depende de leyes y reglamentos, las metas, los objetivos organizacionales, las prácticas de gestión y las políticas de la organización que definen los parámetros, dentro de los cuales, el riesgo de la seguridad del proceso de gestión debe respetar.

Hay muchas metodologías que se ocupan de las partes individuales de las necesidades de una organización de gestión de riesgos. Las organizaciones pueden mirar lo que otros dentro de su dominio han utilizado como opciones viables, centrándose en las leyes y reglamentos. Las organizaciones pueden tener el mandato de aplicar las normas específicas para lograr el

[3] Lozano, Javier. Seguridad de la Información. Riesgos. Internet. www.elmayorportaldegerencia.com/ documentos/188-tecnologias-de-informacion-y-comunicación Acceso: (27 de diciembre de 2012)
[4] Alberts, Christopher. Introduction to the Octave approach. Internet. www.itgovernanceusa.com/files/ Octave.pdf Acceso: (10 de enero de 2013)

cumplimiento normativo. Además, el tamaño de la organización y los recursos financieros ayudarán a determinar las opciones apropiadas.

"Por ejemplo, la adopción de una norma general de diligencia debida, como la Organización Internacional de Normalización (ISO) 17799, puede ser prohibitivamente costoso y no garantiza que los problemas de seguridad de una organización específica sean abordados"[5]. Cada organización debe entender el riesgo y el plan de protección adecuado.

Un riesgo comprende un evento, la incertidumbre y una consecuencia. El evento básico en el que estamos interesados es una amenaza. La incertidumbre se manifiesta en gran parte de la información que se ha recopilado durante la evaluación.

La incertidumbre se refiere a si existe una amenaza a desarrollar, así como si la organización está suficientemente protegida contra el factor amenaza, en muchas metodologías de riesgo, la incertidumbre se representa con probabilidad de ocurrencia.

Para hacer frente a la incertidumbre inherente a los riesgos, se propone una técnica de análisis sobre la base de la planificación de escenarios.

Por último, la consecuencia que en definitiva importa en el riesgo de seguridad de la información, es el impacto resultante en la organización debido a una amenaza. El impacto describe cómo la organización podría verse afectada según los resultados de las siguientes amenazas:

- Revelación de un activo crítico
- Modificación de un activo crítico
- Pérdida / destrucción de un activo crítico
- Interrupción de un activo crítico[6]

Los resultados mencionados anteriormente están directamente relacionados con los activos y describen el efecto de la amenaza sobre un activo.

[5] Woody, Carol, PhD. Applying Octave: Practitioners report. CMU/SEI-2006-TN-010,(Mayo 2006) Pittsburg PA, 2006

[6] Alberts, Christopher. Managing Information Security Risks: The Octave Approach. Estados Unidos, Addison-Wesley Professional, 2002, 123-127

El enfoque OCTAVE utiliza una valoración de evaluación de riesgos basada en los activos. El riesgo de seguridad debe ser considerado cuidadosamente sobre la base de las vulnerabilidades organizacionales y tecnológicas que ponen en peligro a un grupo de activos. Al tener en cuenta más que sólo las vulnerabilidades tecnológicas que un conjunto de herramientas de hardware puede identificar una organización e infraestructura de software, el enfoque OCTAVE aborda las siguientes preguntas:

¿Qué activos requieren protección?

¿Qué nivel de protección se necesita?

¿Cómo podría estar en peligro un bien?

¿Cuál es el impacto si la protección falla?[7]

Un enfoque completo de evaluación del riesgo cuenta con las siguientes características:

- Incorpora activos, amenazas y vulnerabilidades
- Permite a las personas encargadas de tomar decisiones establecer prioridades sobre la base de lo que es importante para la organización
- Incorpora las cuestiones de organización relacionadas con ¿cómo la gente usa la infraestructura de computación para satisfacer los objetivos de negocio de la organización?
- Incorpora aspectos tecnológicos relacionados con la configuración de la infraestructura informática
- Se debe utilizar un método flexible que puede ser usado específicamente en función de cada organización[8]

Mediante el uso de un enfoque equilibrado que combina consideraciones tecnológicas con otras organizaciones, a través de un segmento razonable de la organización, la cual debe ser capaz de evitar sobreproteger algunas áreas mientras que baje el nivel de protección de los demás.

[7] Dorofee, Audrey. Asset-Based information security risk assessments, Cutter Consortium, Enterprise Risk Management and Governance Executive Report. Vol. 2, No. 6. (Marzo 2009)Arlington MA, 2009

[8] Alberts, Christopher. Managing Information Security Risks: The Octave Approach. Estados Unidos, Addison-Wesley Professional, 2002, 118

La figura 1 proporciona una representación humorística pero frecuentemente cierta de la gestión de seguridad de la información en una organización que sólo considera una parte de los riesgos de seguridad que pueden afectar a su organización.

Figura 1: Administración de riesgos de seguridad no balanceado

Realizado por: Bieber, David. The critical success factor method. Internet. www.cert.org/archive/pdf/04tr010.pdf Acceso (24 de enero de 2013)

Actualmente, los riesgos informáticos deben ser considerados dentro del contexto del negocio y dado que cada organización tiene una misión, se debe considerar en ella, la administración del riesgo informático, pues juega un rol crítico y fundamental que contribuye y sustenta el cumplimiento de las metas institucionales.

1.2 Análisis de Seguridades

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones, mediante diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido solo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

Actualmente, la información es el objeto de mayor valor para las empresas, con el avance y progreso de la informática y las redes de comunicación se presenta un nuevo escenario, donde "los objetos del mundo real se representan por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y, en muchos casos, llegando a tener un valor superior."[9]

Por esto y otros motivos, la seguridad de la información es un asunto tan importante para todos, pues afecta directamente a los negocios de una empresa. La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice.

Seguridad de la información es mucho más que la instalación de un firewall, la aplicación de parches para reparar las vulnerabilidades recientemente descubiertas en el software del sistema o cerrar con seguro la caja con sus cintas de copia de seguridad. Seguridad de la información es determinar lo que hay que proteger y por qué, lo que necesita ser protegido de, y cómo proceder durante el tiempo que exista una amenaza.[10]

El propósito de un análisis de seguridad es el proteger los elementos que forman parte de la comunicación, por lo que es necesario identificar los elementos un análisis de seguridad debe proteger:

[9] Rosero, Efraín y Lozano, Javier. Introducción a la seguridad de la información. Internet. www.elmayorportaldegerencia.com/index.php/documentos/188-tecnologias-de-informacion-y-comunicacion/ Acceso: (20 de enero de 2013)

[10] Alberts, Christopher. Managing Information Security Risks: The Octave Approach. Estados Unidos, Addison-Wesley Professional, 2002, 5

- La información
- Los equipos que la soportan
- Las personas que la utilizan[11]

El análisis de seguridad tiene como objetivo: proteger a los activos de una empresa con base en la preservación de tres principios básicos:

Integridad: garantiza que la información no haya sido alterada en su contenido y que por lo tanto, sea íntegra. Una información es íntegra, cuando no ha sido alterada de forma indebida o no autorizada. Cuando ocurre una alteración no autorizada de la información en un documento, quiere decir que el documento ha perdido su integridad, la integridad de la información es fundamental para el éxito de la comunicación.

Buscar la integridad es asegurarse que sólo las personas autorizadas puedan hacer alteraciones en la forma y contenido de una información, así como en el ambiente en el cual, es almacenada y por el cual transita, es decir, en todos los activos. Por lo tanto, para garantizar la integridad, es necesario que todos los elementos que componen la base de gestión de la información se mantengan en sus condiciones originales definidas por sus responsables y propietarios. En resumen, garantizar la integridad es uno de los principales objetivos para la seguridad de la información, de un individuo o de una empresa.

Confidencialidad: el principio de la confidencialidad de la información tiene como propósito asegurar que exclusivamente la persona correcta, acceda a la información que queremos distribuir. La información que se intercambia entre individuos y empresas, no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos y muchas veces, a una única persona. Eso significa que estos datos deberán ser conocidos solo por un grupo controlado de personas, definido por el responsable de la información.

[11] Rosero, Efraín y Lozano, Javier. Introducción a la seguridad de la información. Internet. www.elmayorportaldegerencia.com/index.php/documentos/188-tecnologias-de-informacion-y-comunicacion/ Acceso: (20 de enero de 2013)

La pérdida de confidencialidad, implica pérdida de secreto, si una información es confidencial, es secreta, se deberá guardar con seguridad y no deberá ser divulgada para personas no autorizadas. Garantizar la confidencialidad es uno de los factores determinantes para la seguridad y una de las tareas más difíciles de implementar, pues involucra a todos los elementos que forman parte de la comunicación de la información, desde su emisor, el camino que ella recorre, hasta su receptor. Se deberá considerar a la confidencialidad, con base en el valor que la información tiene para la empresa o la persona y los impactos que podría causar su divulgación indebida. Siendo así, debe ser accedida, leída y alterada solo por aquellos individuos que poseen permisos para ejecutar tales acciones. El acceso debe ser considerado con base en el grado de sigilo de las informaciones, pues no todas las informaciones sensibles de la empresa son confidenciales. Pero para poder garantizar lo anterior, solo la confidencialidad de las informaciones no es suficiente, es importante que además de ser confidenciales, las informaciones también deben ser íntegras. Por lo tanto, se debe mantener la integridad de una información, según el principio básico de la seguridad de la información.

Disponibilidad de la información: una vez que está asegurado que la información correcta llegue a los destinatarios o usuarios correctos, se debe garantizar que llegue en el momento oportuno. Para que una información se pueda utilizar, deberá estar disponible, esto se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento. La disponibilidad de la información permite que: se utilice cuando sea necesario, que esté al alcance de sus usuarios y destinatarios y que se pueda acceder en el momento en que necesitan utilizarla.

Este principio está asociado a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de los negocios de la empresa o de las personas, sin impactos negativos para la utilización de las informaciones. No es suficiente que esté disponible: la información deberá estar accesible, en forma segura para que se pueda usar en el momento en que se solicita y que se garantice su integridad y confidencialidad.

Para que se pueda garantizar la disponibilidad de la información, es necesario conocer cuáles son sus usuarios, con base en el principio de la confidencialidad, para que se puedan organizar

y definir las formas de colocación en disponibilidad, garantizando, conforme el caso, su acceso y uso cuando sea necesario. La disponibilidad de la información se deberá considerar con base en el valor que tiene la información y en el impacto resultante de su falta de disponibilidad.

Mucha gente parece estar buscando una solución mágica cuando se trata de seguridad de la información. Muchas veces se espera que la compra de una herramienta o pieza de tecnología pueda resolver los problemas de la empresa. Pocas organizaciones se detienen a evaluar lo que realmente están tratando de proteger (y por qué) desde una perspectiva organizacional, antes de seleccionar soluciones.

Los problemas de seguridad tienden a ser complejos y rara vez se resuelven simplemente mediante la aplicación de una pieza de tecnología.

La mayoría de los problemas de seguridad están firmemente arraigados en uno o más aspectos organizativos y de negocio. Antes de implementar soluciones de seguridad, se debe considerar la caracterización de la verdadera naturaleza de los problemas de fondo mediante la evaluación de sus necesidades de seguridad y riesgos en el contexto de su negocio.[12]

Teniendo en cuenta las variedades y las limitaciones de los métodos actuales de evaluación de la seguridad, es fácil confundirse cuando se trata de seleccionar un método apropiado para la evaluación de riesgos de seguridad de la información.

"La mayoría de los métodos actuales son 'bottom-up' - que empiezan con la infraestructura informática y centrarse en las vulnerabilidades tecnológicas, sin tener en cuenta los riesgos para la misión de la organización y los objetivos de negocio."[13]

Una mejor alternativa es comenzar con la propia organización y determinar lo que hay que proteger, por lo que está en riesgo y desarrollar soluciones que garanticen su disponibilidad.

[12] Alberts, Chrisptoher. Security Risk Analysis with Octave. Internet. www.informit.com/articles/ Acceso: (25 de enero de 2013)
[13] Alberts, Chrisptoher. Security Risk Analysis with Octave. Internet. www.informit.com/articles/ Acceso: (25 de enero de 2013)

Una evaluación cuidadosa de las necesidades de seguridad y riesgos en este contexto más amplio, debe preceder a cualquier implementación de seguridad para asegurarse de que todos los problemas pertinentes, subyacentes son primero descubiertos.

El enfoque OCTAVE para las evaluaciones de seguridad auto-dirigidos fue desarrollado en el Centro de Coordinación CERT. Este enfoque está diseñado para:

- Identificar y clasificar los activos de información clave
- Pese a las amenazas de esos activos, analizar las vulnerabilidades que implican la tecnología y las prácticas[14]

OCTAVE permite a cualquier organización desarrollar las prioridades de seguridad basada en las preocupaciones de la organización de negocios particulares. Este enfoque proporciona un marco coherente para alinear las acciones de seguridad con los objetivos generales.

El primer paso en el ciclo de seguridad de la información, es identificar las distintas amenazas de las que pueden ser víctimas las empresas, poder identificar estas amenazas, permite que se conozca los puntos débiles de los activos de la organización.

Esta exposición lleva a la pérdida de uno o más principios básicos de la seguridad de la información, causando impactos en el negocio de la empresa, aumentando aun más los riesgos a los que está expuesta la información. Para que el impacto de estas amenazas al negocio se pueda reducir, se toman medidas de seguridad para impedir la ocurrencia de puntos débiles.[15]

[14] Alberts, Chrisptoher. Security Risk Analysis with Octave. Internet. www.informit.com/articles/ Acceso: (25 de enero de 2013)

[15] Cevallos Pablo. Introducción a defensa en profundidad y seguridad de la información TI. Internet. www.repositorio.utn.edu.ec Acceso: 27 de enero de 2013

Figura 2: Ciclo de seguridad de la información

Realizado por: Cevallos Pablo. Introducción a defensa en profundidad y seguridad de la información TI. Internet. www.repositorio.utn.edu.ec Acceso: 27 de enero de 2013

Los distintos problemas en la seguridad de la empresa aumentan en la medida que las amenazas pueden explotar las vulnerabilidades y por tanto, causar daño en los activos. Estos daños pueden causar que la confidencialidad, integridad o disponibilidad de la información se pierda, causando impactos en el negocio de la empresa.

Las medidas de seguridad permiten disminuir los riesgos, y con esto, permitir que el ciclo sea de mucho menor impacto para los activos y la empresa.

El propósito de un análisis de seguridad es:

- Proteger a los activos contra accesos no autorizados.
- Evitar alteraciones indebidas que pongan en peligro su integridad.
- Garantizar la disponibilidad de la información.[16]

[16] Cevallos Pablo. Introducción a defensa en profundidad y seguridad de la información TI. Internet. www.repositorio.utn.edu.ec Acceso: 27 de enero de 2013

1.3 Justificación del uso de la Norma

A continuación se presenta un cuadro comparativo entre Octave-S, ISO 17799 y Cobit versión 4.1:

Tabla 1: Análisis comparativo entre la norma Octave-S, norma ISO 17799 y Cobit 4.1

Octave – S **Operationally Critical Threats, Assets and Vulnerability Evaluation** [17]	**ISO 17799** **Sistema de Gestión de Seguridad de la Información**[18]	**COBIT** **Control Objectives for Information and Related Technologies** [19]
Es una aproximación al manejo de riesgos en seguridad informática. Es una suite de herramientas, técnicas y métodos de evaluación que sirven de guía en la planificación estratégica basada en el riesgo y la seguridad de la información. Los aspectos organizativos, tecnológicos y el análisis de riesgos de seguridad de información se complementan, lo que permite al personal de la organización tener una imagen completa de las necesidades de seguridad de la información en la organización. Enfocado para pequeñas y medianas empresas.	Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización. Define la información como un activo que posee valor para la organización y requiere una protección adecuada. Es un acercamiento sistemático para manejar la información y la propiedad confidencial de una compañía para mantenerlas seguras. Abarca personas, procesos de negocio e instalaciones de procesamiento de información**.**	Es un conjunto de mejores prácticas para el manejo de información, mediante la investigación, el desarrollo y promover y hacer público un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de los Gerentes de negocio y profesionales de TI, permite el desarrollo de políticas claras y de buenas prácticas para el control de TI por parte de la empresa. Las buenas prácticas centradas en el marco de referencia COBIT, permiten que los negocios se alineen con la tecnología de la información para alcanzar los mejores resultados.

[17] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 5-28
[18] Guayaquil, Nidia. "Estándar ISO 1779 y Norma ISO 27001",2, (21 de septiembre de 2007), Quito, 2007: 3-31
[19] Mc Leod, Joel. Octave Method. Internet. www.cert.org/octave Acceso: 17 de diciembre de 2013

Características:
• Es un análisis o valoración de riesgos que permite estar en capacidad de:
  ○ Identificar, evaluar y manejar los riesgos de seguridad informática
  ○ Establecer la probabilidad de que un recurso informático. quede expuesto a un evento y el impacto en la organización.
  ○ Determinar las medidas de seguridad que minimizan o neutralizan el riesgo a un costo razonable.
  ○ Tomar decisiones preventivas y planeadas en seguridad.
• Diferente de los análisis tradicionales enfocados a tecnología.
• Auto dirigido: ya que pequeños equipos de personal de la organización en todas las unidades de
	Características:
	• Trata de definir el manejo de riesgo de una empresa.
	• Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).
	• Basado en ciclo Deming (Planear, Hacer, Revisar, Actuar).
	• La seguridad de la información es una medida para incrementar el éxito de los negocios.
	• El implementar un Sistema de Gestión de la Seguridad de la Información, puede ayudar a que una organización cumpla favorablemente los incentivos de mercadotecnia, los financieros y las oportunidades de crecimiento.
	• Protege adecuadamente los activos para asegurar la continuidad del negocio.
	• Minimiza los daños a la organización.
	• Maximiza el retorno de las
		Características:
		• Orientado al negocio. COBIT está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio. El marco de trabajo COBIT se basa en el siguiente principio: Para proporcionar la información que la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida. Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de información del negocio: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.
		• Orientado a procesos. COBIT define las actividades de TI en un modelo genérico de treinta y

negocio y de TI trabajan juntos para hacer frente a las necesidades de seguridad de la organización. • Flexible: porque 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. • Evolucionado: OCTAVE trasladó a la organización hacia una vista y funcionamiento operacional basada en los riesgos y la seguridad y se enfoca en la tecnología en un contexto del negocio	inversiones y las oportunidades de negocio. • Proporciona una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.	cuatro procesos organizado en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar • Basado en controles. COBIT define objetivos de control para los treinta y cuatro procesos, así como para el proceso general y los controles de aplicación. • Impulsado por la medición. Una necesidad básica de toda empresa, es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para poder tener una visión objetiva del nivel de desempeño de una empresa COBIT ha desarrollado modelos de madurez, metas y mediciones de desempeño para los procesos de TI y metas de actividades.
Equipo: • Identificar recursos importantes. • Enfocar las actividades de análisis de riesgos. • Relacionar amenazas y vulnerabilidades. • Evaluar riesgos. • Crear una estrategia de	**Equipo:** • Proteger adecuadamente los activos para asegurar la continuidad del negocio. • Minimizar los daños a la organización. • Maximizar el retorno de inversiones. • Proporcionar una base	**Equipo:** • Mantener información de alta calidad para apoyar las decisiones de negocios. • Mantener los riesgos relacionados a TI bajo un nivel aceptable. • Optimizar los servicios el coste de las TI y tecnología.

protección.	común para desarrollar normas de seguridad.	• Apoyar el cumplimiento de las leyes, reglamentos y acuerdos.

Componentes:
• Los elementos que el análisis de riesgos debe cubrir son:
  ○ Análisis de los activos que son de valor.
  ○ Análisis de amenazas cuya ocurrencia pueda producir pérdidas a la organización.
  ○ Análisis de vulnerabilidades en los controles de seguridad de los sistemas
  ○ Análisis de todos los riesgos y sus impactos en las operaciones de la organización.
  ○ Análisis de las medidas de seguridad que actuarían como un escudo de protección total o parcial contra cada riesgo.
• Principios
• Atributos
	Componentes:
	• Basado en el modelo de la gestión de la seguridad:
	  ○ Política de Seguridad de la Información.
	  ○ Organización de la Seguridad de la Información.
	  ○ Gestión de Activos de Información.
	  ○ Seguridad de los Recursos Humanos.
	  ○ Seguridad Física y Ambiental.
	  ○ Gestión de las Comunicaciones y Operaciones.
	  ○ Control de Accesos.
	  ○ Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
	  ○ Gestión de Incidentes en la Seguridad de la Información.
	  ○ Gestión de Continuidad del
		Componentes:
		• Áreas de enfoque del Gobierno de TI
		• Metas de negocio
		• Metas de TI
		• Indicadores de rendimiento
		• Recursos de TI
		• Dominios COBIT
		  ○ Planear y Organizar
		  ○ Adquirir e Implementar
		  ○ Entregar y Dar Soporte
		  ○ Monitorear y Evaluar
		• Procesos COBIT
		• Objetivos de Control

• Salidas	Negocio. o Cumplimiento.	
Método Octave – S • Fase 1: o Identificar información de la organización. o Crear perfiles de amenazas. • Fase 2: o Examinar infraestructura tecnológica y su relación con los bienes críticos. • Fase 3: o Identificar y analizar riesgos. o Desarrollar estrategias de mitigación de planes de protección.	**Aplicación de la Norma:** • Auditoria: o Valoración del nivel de adecuación, implantación y gestión en: seguridad lógica, física, organizativa y legal. • Consultoría: o Conociendo el nivel de cumplimiento actual, se debe determinar el nivel mínimo aceptable y el nivel objetivo en la organización. • Implantación	**Implantación COBIT:** • Establecer principios y objetivos. • Identificar áreas de enfoque. • Implantar de acuerdo a los procesos críticos para el negocio. • Elaborar herramientas de apoyo COBIT: o Encuestas o Matrices de Madurez o Val IT o Herramientas automáticas • Planificar mejoras de control. • Conclusiones y Recomendaciones
Resultados: • Estrategia de protección (define el rumbo de la organización). • Plan de mitigación (diseñado para reducir el riesgo). • Lista de acción (acciones a corto plazo).	**Resultados:** • Certificación ISO 27001: requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la información según el Ciclo Deming.	**Resultados:** • Refleja un amplio rango de buenas y mejores prácticas. • Certificaciones: o CISA o CISM. o CGEIT o CRISC

Después de implementado: • Plan de acción • Monitoreo • Control	**Después de implementado:** • Proceso de mejora continua. • Plan de acción • Monitoreo y Control	**Después de implementado:** • Proceso de mejora continua. • Plan de acción • Monitoreo y Control

Realizado por: Olga Páez

Del cuadro anterior se desprenden las siguientes conclusiones:

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.

Utiliza un método de taller auto-dirigido en el que un equipo formado por distintas personas que trabajan en la empresa, jefes operativos de personal, de seguridad y se analiza una serie de escenarios, cuestionarios y listas de verificación. Los escenarios 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.

Se escogió OCTAVE-S para implementarlo en la empresa Pirámide Digital Cía. Ltda., por cuanto después de una reunión explicativa y de coordinación con el Gerente General de esta empresa, luego de analizar las tres metodologías expuestas en la Tabla 1 de esta Tesis, se decidió que el método que propone OCTAVE-S, 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.

CAPITULO DOS

ANALISIS DE LA SITUACION ACTUAL DE LA EMPRESA

2.1 Justificación del uso del modelo Cobit versión 4.1

En base a la Tabla 1 presentada en el Capítulo Uno, se seleccionó Cobit 4.1 como el modelo para realizar el análisis de la situación actual de la empresa Pirámide Digital Cía. Ltda. en base al framework de mejores prácticas de Cobit 4.1, dirigida a la gestión de tecnología de la información de la empresa.

En la actualidad, los gerentes de negocio y profesionales de TI están interesados en aplicar un marco de trabajo actualizado, autorizado, fácil de utilizar diariamente y aceptado internacionalmente, es por esto que el modelo que propone Cobit se puede orientar a todos los sectores de una organización y sirve para auditar la gestión de control de los sistemas de información.

Los principales beneficios de implementar Cobit 4.1 son:

- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores.
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI.[20]

2.1.1 Marco de Trabajo Cobit 4.1

2.1.1.1 Misión de Cobit

Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento[21].

[20] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 8
[21] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 9

2.1.1.2 Áreas de enfoque del Gobierno de TI

Cada área de enfoque que propone Cobit describe distintos temas que la dirección ejecutiva de la empresa debe tomar en cuenta y prestar más atención, enfocándose en los requerimientos para lograr una administración y control adecuado de TI, las cinco áreas de enfoque son:

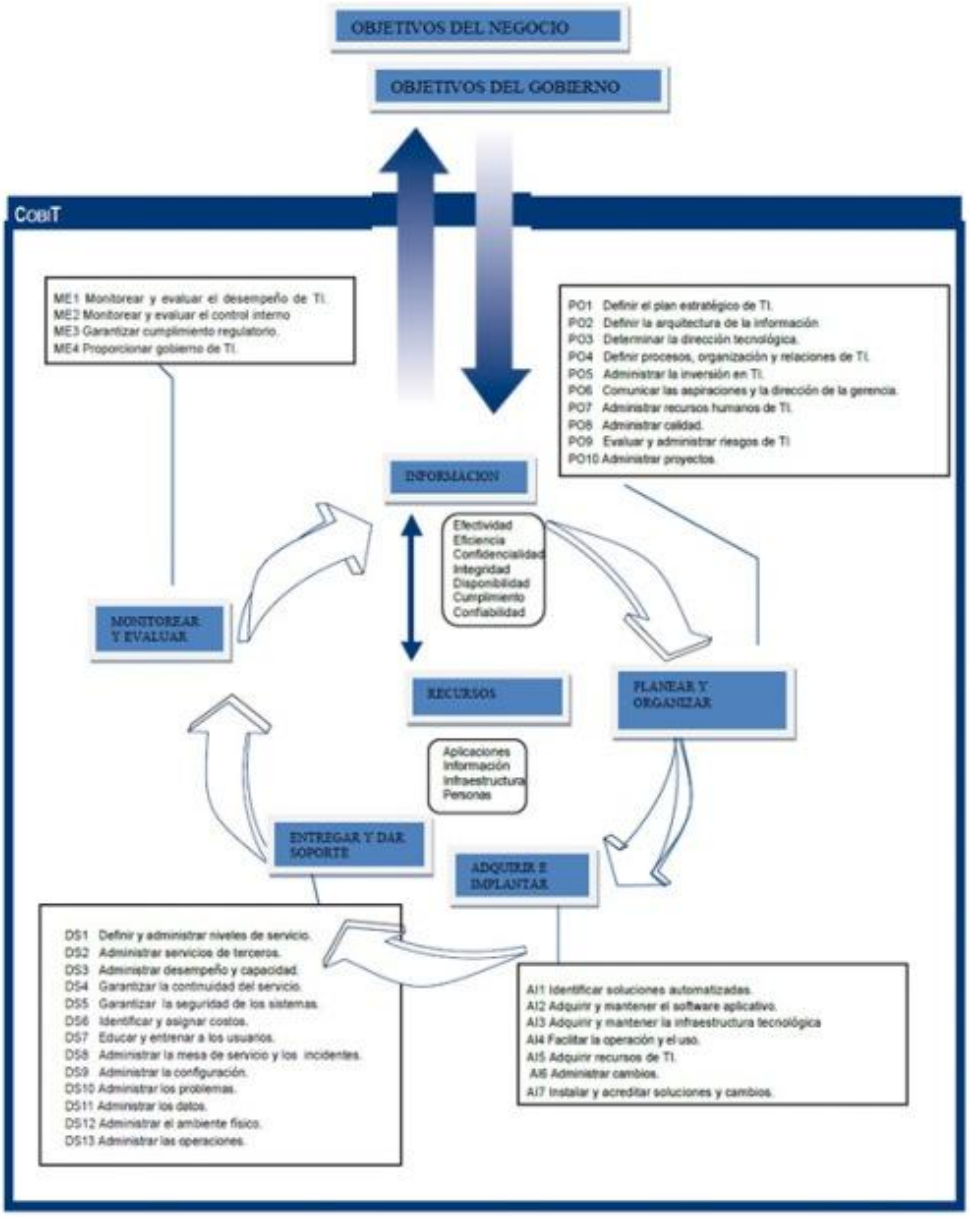
- **Alineación estratégica:** se enfoca en garantizar la alineación entre los planes de negocio y de TI: en definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la empresa.
- **Entrega de valor:** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos.
- **Administración de recursos:** se trata de la inversión óptima, asi como en la administración adecuada de los recursos críticos de TI (aplicaciones, información, infraestructura y personas).
- **Administración de riesgos:** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento de los requerimientos de cumplimiento, trasparencia de los riesgos significativos para la empresa y la inclusión de las responsabilidades de administración de riesgo dentro de la organización.
- **Medición del desempeño:** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio. [22]

2.1.1.3 Marco general de trabajo Cobit 4.1

Se define un modelo que divide el área de TI en treinta y cuatro procesos alineados con las áreas de planificar y organizar, adquirir e implementar, entrega y soporte y monitorear y evaluar, proveyendo una visión de principio afín de TI.

[22] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 6

Figura 3: Marco de trabajo general de Cobit 4.1



Realizado por: Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 26

Cobit define las actividades de TI en un modelo de procesos que pertenecen a cuatro dominios:

- **Planear y Organizar (PO):** este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio.
- **Adquirir e Implementar (AI):** para realizar la estrategia de TI, se necesita identificar soluciones de TI y también implementarlas e integrarlas en el proceso de negocio.
- **Entrega y Soporte (DS):** este dominio trata de la entrega en sí de los servicios requeridos, lo cual incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.
- **Monitorear y Evaluar (ME):** todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y de cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y el gobierno de aprovisionamiento. [23]

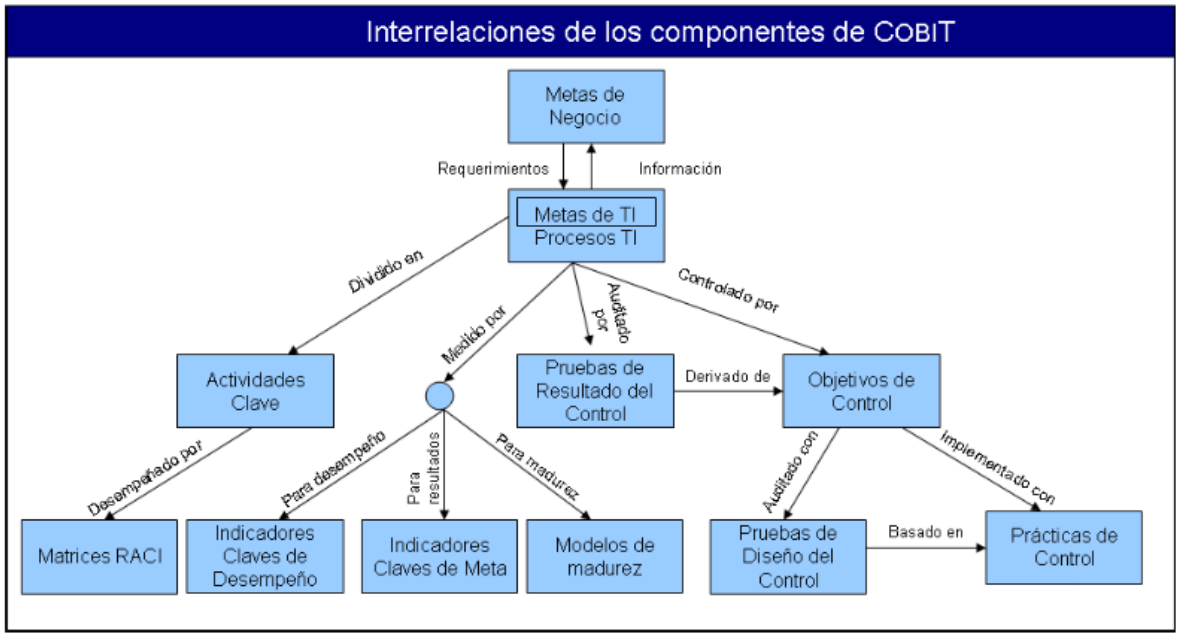
Los cuatro dominios propuestos por Cobit están divididos en treinta y cuatro procesos y más de trescientos objetivos de control.

2.1.2 Interrelaciones de los componentes Cobit 4.1

Los recursos de TI están gestionados por los procesos de TI para alcanzar las metas de TI que responden y se alinean a los requerimientos del negocio.

[23] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 12-13

Figura 4: Interrelaciones de los componentes Cobit 4.1



Realizado por: Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 8

Los beneficios de implementar Cobit son:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI[24]

[24] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 8

2.1.3 Criterios de información de Cobit 4.1

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en Cobit como requerimientos de información del negocio. Con base a los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- **Efectividad:** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- **Eficiencia:** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- **Confidencialidad:** se refiere a la protección de información sensitiva contra revelación no autorizada.
- **Integridad:** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- **Disponibilidad:** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- **Cumplimiento:** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- **Confiabilidad:** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.[25]

[25] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 10-11

2.1.4 Metas de negocio y de TI

La definición de un conjunto de metas de negocios y TI sirven para contar con una base que ayude a establecer requerimientos de negocios y desarrollar métricas que permitan la medición de estas metas. Cada empresa usa TI para soportar iniciativas de negocios y estas pueden estar representadas como metas de negocio para TI. Si TI va a entregar exitosamente servicios para soportar la estrategia de la empresa, debería haber una propiedad y dirección claras de los requerimientos para el negocio (el cliente) y un claro entendimiento de qué necesita ser entregado y como por parte de TI (el proveedor).

2.1.5 Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. "Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada."[26]

Los recursos de TI identificados en COBIT 4.1 se definen:

- **Aplicaciones:** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **Información:** son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- **Infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- **Personas:** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran. [27]

[26] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007,11
[27] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007,12

2.2 Caracterización de la Empresa

2.2.1 Misión

"Proveer al mercado latinoamericano, de las más efectivas herramientas para optimizar la gestión gerencial, mediante soluciones integrales de alta calidad, con tecnología de punta y un equipo profesional altamente capacitado."[28]

2.2.2 Visión

"Ser y ser considerados como la empresa líder en el mercado latinoamericano, en consultoría y capacitación para la alta gerencia."[29]

2.2.3 Valores

- Responsabilidad
- Cultura de servicio
- Compromiso
- Constancia
- Respeto a la dignidad humana
- Trabajo en equipo
- Comunicación
- Ética empresarial
- Confianza en la palabra[30]

2.2.4 Descripción histórica

Pirámide Digital Cía. Ltda. empresa ecuatoriana fundada en el año 2003, conformada por un equipo de gente joven, dinámica y actualizada, enfocada en desarrollar las capacidades que exige cada persona en cada organización.

Comprometidos con el desarrollo integral de sus clientes. Trabajando siempre con los más altos estándares de calidad y eficiencia y con el más profundo respeto al ser humano;

[28] Entregado por la empresa Pirámide Digital Cía. Ltda.
[29] Entregado por la empresa Pirámide Digital Cía. Ltda.
[30] Entregado por la empresa Pirámide Digital Cía. Ltda.

garantizando al cliente confidencialidad total en cuanto a sus proyectos, realidades, situaciones y desempeño.

Pirámide Digital fue la primera empresa ecuatoriana especializada en ofrecer soluciones de capacitación y consultoría, ajustadas a las necesidades de sus clientes.

Su experiencia y habilidades en las áreas de desarrollo de estrategias, reestructuración de procesos y organizaciones, desarrollo de sistemas de servicios y promoción de habilidades gerenciales, los colocan como los únicos en el mercado ecuatoriano con la capacidad de ofrecer soluciones y resultados realmente alineados con las estrategias, planes y metas de su negocio, hablando el mismo idioma que su equipo directivo y conociendo las implicaciones de negocio, envueltas en cada decisión de desarrollo.

Para ello, cuentan con un equipo de profesionales altamente calificado, con experiencia práctica nacional e internacional y excelente preparación académica; formados en metodologías de aprendizaje y cambio organizacional, quienes proveen la mezcla perfecta para garantizar la transferencia de conocimientos y la aplicabilidad de las soluciones. De hecho, han tenido la oportunidad de prestar sus servicios profesionales, de capacitación y de consultoría en más de quince países alrededor del mundo.

Otra de sus fortalezas, es la flexibilidad en sus proyectos y programas, ya que diseñan las soluciones de manera particularizada, de acuerdo a las necesidades y circunstancias específicas de cada empresa, de cada cliente.

Su metodología de trabajo se basa en comprender que cada cliente es único y especial. Las soluciones enlatadas no son una opción y sus historias de éxito así lo demuestran.

Un principio fundamental que guía su trabajo, es transferir las habilidades, destrezas y conocimientos a sus clientes de forma práctica y aplicable, logrando que sean capaces de continuar su crecimiento de manera independiente.

2.2.5 Actividades principales

Todos los programas de capacitación y de consultoría que ofrece Pirámide Digital, se diseñan de acuerdo al objetivo empresarial y de aprendizaje del cliente y considerando el perfil de las personas que van a participar y las metas que se pretenden conseguir.

Para cumplir con sus objetivos, se ha diseñado una plataforma de servicios que incluye:

***Cursos gerenciales on-line*:** Pirámide Digital tiene implementado desde hace más de un año este servicio, como una nueva opción metodológica de capacitación, basada en el uso de tecnología de punta: Servicios de Capacitación Gerencial On-Line.

La idea que sustenta este servicio es que los objetos de aprendizaje tienen sus orígenes en la programación, diseño, análisis y teorías orientadas a objetos.

Los Cursos de Entrenamiento y Capacitación Gerencial On-Line, que actualmente ofrece Pirámide Digital, son los siguientes:

- Liderazgo Ejecutivo para la Alta Gerencia
- Convergencia Tecnológica
- Estrategia
- Gerencia
- Gerencia de IT
- Plan de Mercadeo
- Sistemas de Información Gerencial
- Tecnologías de Información y Comunicación
- Otros temas gerenciales

***Cursos gerenciales presenciales*:** están focalizados en atender y solucionar aspectos puntuales o áreas específicas de crecimiento o mejora, pues entendemos al negocio como un conjunto de variables sobre las que se hace necesario tomar control y optar por las decisiones más oportunas.

Dentro del esquema de capacitación presencial, nuestro paquete de servicios, incluye aproximadamente cien Cursos Gerenciales, divididos en seis grandes grupos:

Simuladores de Negocios:

- Modelo de Simulación de Negocios - General
- Modelo de Simulación de Negocios - Eléctricas
- Modelo de Simulación de Negocios - Petróleo
- Modelo de Simulación de Negocios – Telecomunicaciones
- Modelo de Simulación de Negocios - A la medida de sus necesidades

CRM – Customer Relationship Management:

- Servicio al Cliente de Clase Mundial
- Estrategias Exitosas de Implementación de CRM
- Gerencia Operativa de Centros de Contacto
- Estrategias Efectivas de Cierres de Ventas y Manejo de Objeciones
- Cursos Gerenciales de CRM a la Medida de sus Necesidades

Interés Gerencial:

- Coaching para Líderes
- Gerencia del Desempeño y Balanced Scorecard
- Emprendedor Electrónico
- Gerencia con Programación Neurolinguística (PNL)
- Cursos de Interés Gerencial a la Medida de sus Necesidades

Desarrollo de Ejecutivos:

- Diplomado en Gerencia de Centros de Contacto
- Administración Efectiva del Tiempo
- Competencias del Capital Humano
- Formando Líderes Exitosos en su Empresa

- Cursos Gerenciales de Desarrollo de Ejecutivos a la Medida de sus Necesidades

Telecomunicaciones, Tecnología y Utilities:

- Estrategias Exitosas de Ventas, Retención y Fidelización para empresas de Telecomunicaciones
- Modelo de Simulación de Negocios aplicado a las Telecomunicaciones
- Modelo de Simulación de Negocios aplicado a Empresas Eléctricas
- Diplomado en Gerencia de Telecomunicaciones
- Cómo Implementar ERP's Eficientemente
- Gerencia Operativa en Empresas de Telecomunicaciones
- Tecnología para Fóbicos Tecnológicos
- Indicadores Claves de Operación y Rendimiento para Empresas de Telecomunicaciones
- Gerencia de Marketing para Empresas de Telecomunicaciones
- Gerencia Efectiva de Proyectos
- Desarrollo de Planes de Negocios Exitosos para Empresas de Telecomunicaciones
- Gerencia de Redes y Seguridades Informáticas
- Cursos Gerencias de Telecomunicaciones, Tecnología y Utilities a la medida de sus necesidades

***Consultorías en desarrollo organizacional*:** en las que se brinda ayuda ayudar con procesos de:

- Selección de Personal:
    - Búsqueda de talentos
    - HeadHunting
    - Evaluaciones de selección de personal
- Diagnóstico Estratégico Organizacional:
    - Clima organizacional
    - Niveles de satisfacción actual del personal
    - Factores de motivación actual del personal

  - Diagnóstico organizacional en 12 dimensiones
  - Problemas técnicos, administrativos y de relaciones interpersonales
  - Mapeo del recurso humano
- Desarrollo de Habilidades Ejecutivas:
  - Liderazgo
  - Comunicación
  - Trabajo en Equipo
  - Coaching Ejecutivo
- Administración de Nómina:
  - Outsourcing de personal
  - Administración de beneficios y compensaciones
  - Valoración de cargos y competencias
  - Estadísticas Gerenciales
  - Pago de obligaciones laborales
  - Manejo de conflictos
  - Outplacement
  - Indicadores de satisfacción del personal
  - Manejo electrónico de nómina
- Evaluación de Desempeño:
  - Balanced Scorecard
  - Indicadores de Gestión
  - Identificación de competencias de gestión
  - Evaluación de desempeño de 360 grados
- Procesos y Procedimientos:
  - Mapeo de procesos
  - Las 7 herramientas claves de procesos
  - Diagnóstico organizacional en 4 dimensiones
  - Tiempos y movimientos
  - Indicadores financieros y de producción
- Planificación Estratégica:

  - Definición de Objetivos Estratégicos
  - Mapa Estratégico
  - Indicadores Claves de Gestión
  - Indicadores Claves del Negocio
  - FODA
  - Plan Operativo Anual POA
- Certificaciones:
  - ISO
  - COPC

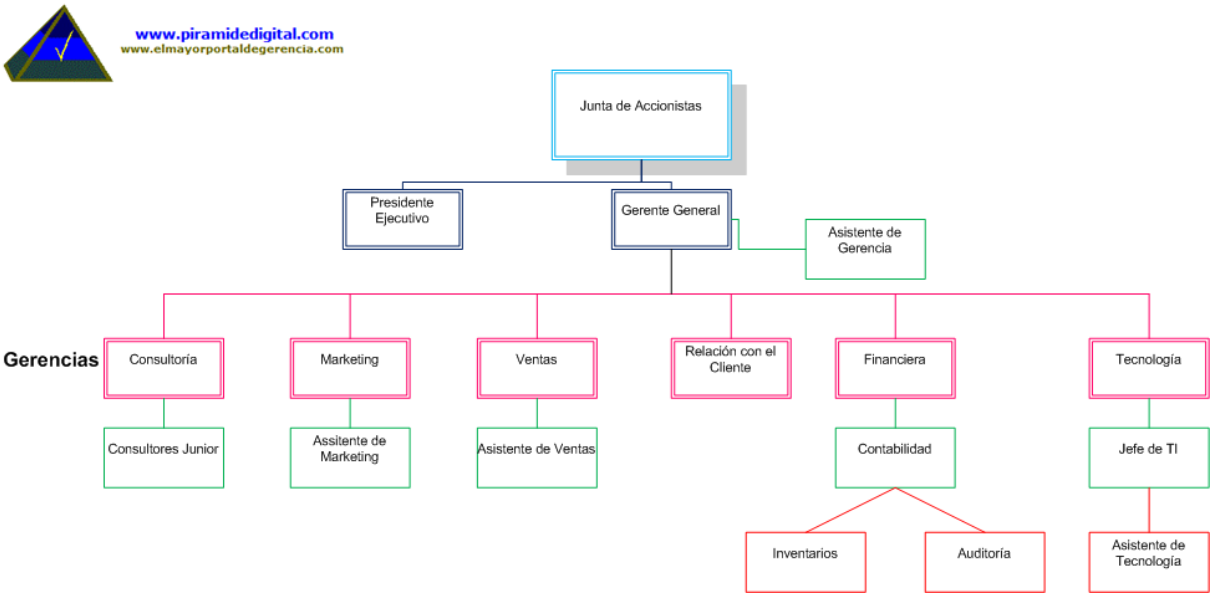
- Consultoría en Desarrollo Organizacional, de acuerdo a sus necesidades y presupuestos

Consultorías de gestión: en las que proveen los servicios de:

- Servicio de Diseño y Rediseño de Procesos
- Análisis de Valor Agregado
- Costeo ABC
- Planificación Estratégica
- Indicadores de Gestión
- Consultoría de Gestión, de acuerdo a sus necesidades y presupuestos

2.2.6 Estructura organizacional

Figura 5: Estructura organizacional empresa Pirámide Digital Cía. Ltda.

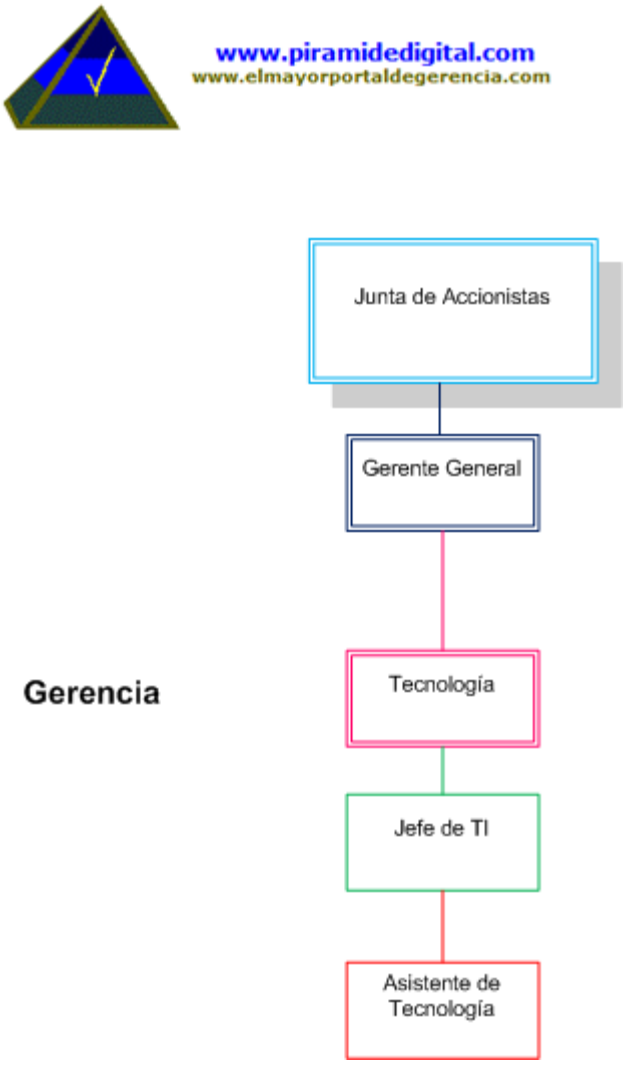


Realizado por: Olga Páez en base a información brindada por Pirámide Digital Cía. Ltda.

De acuerdo al gráfico anterior, se concluye que la ubicación del área de tecnología no es adecuada, ya que debe estar en un nivel de asesoría para poder mejorar el nivel de decisión de la Gerencia de Tecnología.

2.2.7 Estructura de la unidad informática

Figura 6: Estructura de la unidad informática empresa Pirámide Digital Cía. Ltda.



Realizado por: Olga Páez en base a información brindada por Pirámide Digital Cía. Ltda.

2.2.8 Seguridad de la unidad informática

2.2.8.1 Seguridad física

Para poder acceder a las oficinas de la empresa ubicadas en la Avenida 12 de Octubre y Cordero en el Edificio World Trade Center torre B oficina 702, se debe dejar una identificación con el guardia en la planta baja del edificio y dar a conocer el motivo de la visita.

En la oficina principal de la empresa, se encuentra el área administrativa y las gerencias de consultoría, relación con el cliente y financiera. Para poder acceder a documentos de importancia o confidenciales de la empresa, se debe hacer con el respectivo permiso del Gerente General, quien delega que su asistente administrativa nos dé una copia de los documentos requeridos, previo a la firma de un acuerdo de confidencialidad.

En las oficinas ubicadas en Campos Verdes calle Juan Pascoe lote 115 y Miriam de Sevilla en el Valle de los Chillos, se encuentra la Gerencia General, las gerencias de ventas, marketing y tecnología. Para el ingreso al área de sistemas y el cuarto donde se encuentran los servidores, cada persona debe activar el acceso mediante su tarjeta magnética, y siempre el Asistente de tecnología está presente durante la visita.

En el cuarto de servidores se cuenta con:

- Ventilación las 24 horas
- Extinguidores de incendio
- Cinco UPSs

La empresa cuenta dentro de su documentación formal con una ley de políticas de salud, que es un acuerdo firmado por cada empleado en el que se garantiza un servicio de salud preventivo y curativo, así como con un código de conducta en el que se expresa claramente la posición de la empresa en relación con el cumplimiento de las leyes, el respeto a las normas éticas y el compromiso con las personas que forman parte de la compañía y con un acuerdo de confidencialidad que debe firmar todo empleado y se compromete a no divulgar información

delicada de la empresa. También cuenta con un plan de la red de datos en la que se muestra como está estructurada la red dentro del edificio.

2.2.8.2 Seguridad lógica

Para el acceso a cada máquina cliente o servidores, cada usuario cuenta con una clave y contraseña personal, las que deben ser cambiadas cada seis meses por motivos de seguridad.

Para el control de accesos a ambas oficinas, cada empleado cuenta con una identificación con su nombre, cargo y una fotografía y también con una tarjeta magnética para el acceso desde el parqueadero hasta cada una de las oficinas de la empresa.

2.2.8.3 Seguridad legal

Los cinco servidores que tiene la empresa tienen garantía de fábrica en caso de daños o desperfectos, además se cuentan con contratos de mantenimiento y soporte para el servidor principal.

Los servidores, las estaciones de trabajo y periféricos están asegurados en caso de robos o desperfectos.

2.2.8.4 Seguridad de datos

Para proteger adecuadamente los datos, aplicaciones y software residentes en los servidores, se han definido procesos de respaldo cuya ejecución está a cargo del Asistente de Tecnología, debe revisar que los respaldos que se ejecutan automáticamente se hayan hecho adecuadamente y realizar un respaldo manual una vez al mes de la página web de la empresa; además de realizar respaldos diarios del servidor de la base de datos, en caso de que se presente algún problema

Existe una replicación de datos en un servidor alojado en California, Estados Unidos.

2.2.9 Caracterización de la Carga

La empresa cuenta con cinco servidores:

- Servidor mail
- Servidor web
- Servidor proxy
- Servido de bases de datos
- Servidor de seguridad

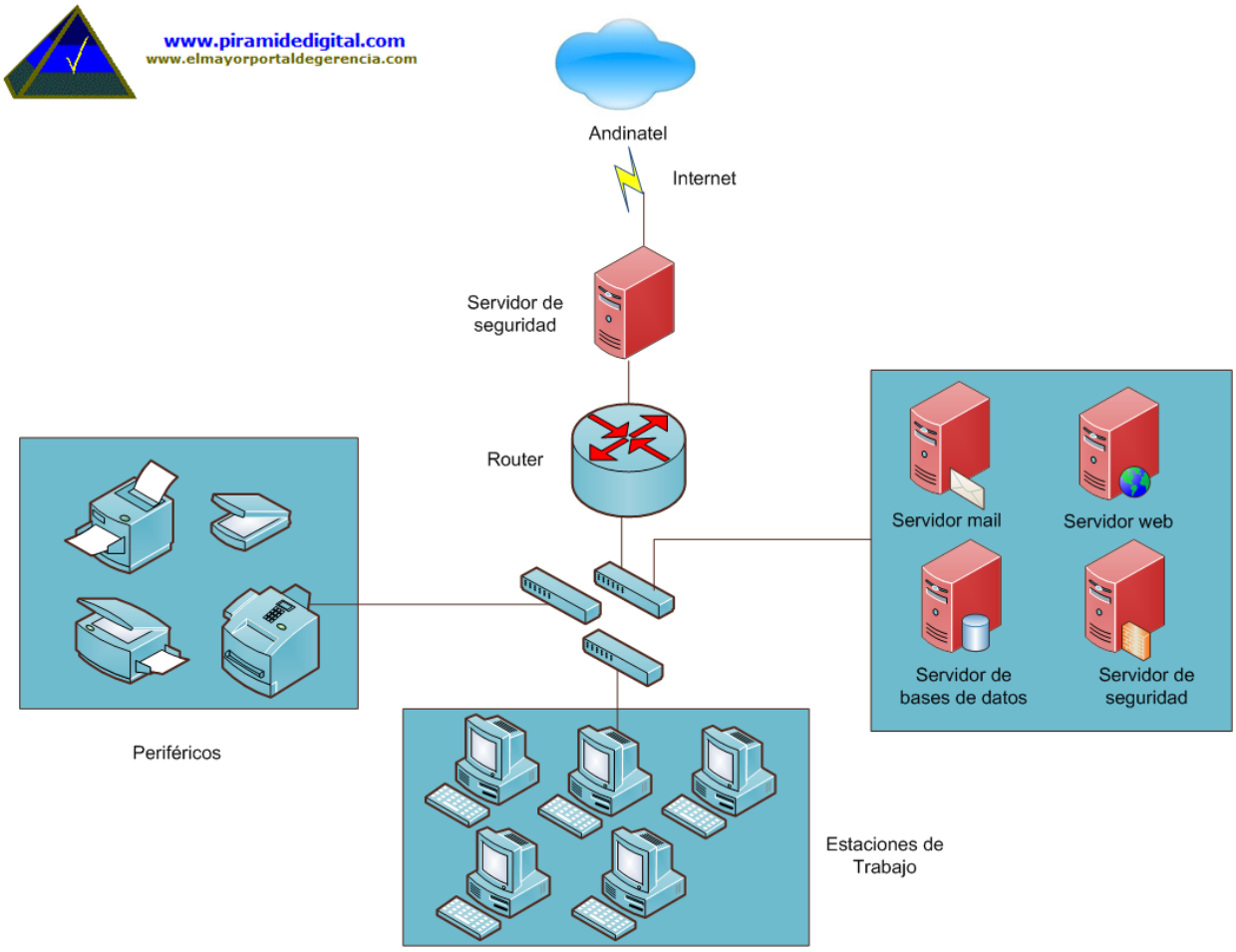
Las actividades en la empresa se realizan de lunes a viernes desde las 9:00 am hasta las 16:00.

2.2.9.1 Topología de red

La empresa Pirámide Digital Cía. Ltda. utiliza el enlace dedicado del proveedor de servicio de internet Andinatel, el que se enlaza con la oficina ubicada en el Valle de los Chillos por medio de la recepción del router a través de una Red Privada Virtual (VPN) para tener acceso a archivos o documentos compartidos y monitorear los servidores desde donde sea que se encuentren.

La empresa cuenta con una conexión de banda ancha de 256 Kbps para ambas oficinas, y como se observa en la siguiente gráfica, para la distribución de información se emplea la siguiente topología de red:

Figura 7: Mapa topológico de red de la empresa Pirámide Digital Cía. Ltda.



Realizado por: Olga Páez en base a información brindada por Pirámide Digital Cía. Ltda.

2.2.9.2 Determinación del periodo más representativo

El instante de tiempo en el que se ha comprobado que los servidores se encuentran atendiendo al mayor número de usuarios durante la jornada de trabajo, está entre las 11:30 am y las 13:00 y después del receso por la hora de almuerzo entre las 15:00 hasta las 16:00.

2.2.9.3 Determinación del tipo de carga

Los cinco servidores tienen carga interactiva, ya que los empleados de la empresa acceden al a cada uno se los servidores para poder hacer uso del servicio, y todos los usuarios interactivos reciben de inmediato el servicio, garantizando buenos tiempos de respuesta.

2.2.9.4 Definición de la etapa de desarrollo de la carga

La etapa de desarrollo de la carga en la que actualmente se encuentra la empresa Pirámide Digital Cía. Ltda. actualmente es de crecimiento, ya que el número de empleados no es mayor, haciendo que la carga sea pequeña y que todos los usuarios reciban un servicio acorde con sus expectativas.

2.3 Aplicación del modelo Cobit 4.1 para realizar un diagnóstico de la situación actual de la empresa

2.3.1 Modelos de Madurez

Cobit 4.1 presenta un modelo de madurez basado en el Modelo de Evolución de Capacidades de Software (CMM), el que establece un "orden claro, discreto y absoluto, definiendo niveles o etapas de madurez"[31] además establece métricas para evaluar el nivel de los controles de TI, los cuales deben ser alineados con el nivel correspondiente de los procesos de TI.

En este modelo se describen cinco niveles de madurez, a través de distintos procesos de madurez desarrollados para los treinta y cuatro procesos de Cobit 4.1, la empresa Pirámide Digital Cía. Ltda. podrá conocer cuál es su desempeño actual y cuál es su objetivo de mejora.

El modelo de madurez se lo utiliza con una escala de medición creciente a partir de cero hasta cinco, el desarrollo de esta escala se describe a continuación:

[31] Arbeláez Roberto. Modelos de madurez de seguridad de la información: cómo debe evolucionar la seguridad en las organizaciones. Internet. www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/05-ModelosMadurezSeguridadInformatica.pdf Acceso: 11 de febrero de 2013

Tabla 2: Modelo de madurez

Nivel	Descripción
0 No existente	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado	Los procesos se han realizado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Realizado por: Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 19

2.3.2 Modelos de madurez de los procesos Cobit 4.1 seleccionados

De acuerdo a los objetivos del proyecto de disertación y previo a una reunión con el Gerente General de Pirámide Digital, se han seleccionado los siguientes procesos de Cobit 4.1:

- PO1: Definir el plan estratégico de TI
- PO3: Determinar la dirección tecnológica
- PO4: Definir procesos, organización y relaciones de TI
- PO9: Evaluar y administrar riesgos de TI
- AI5: Instalar y acreditar sistemas
- AI6: Administrar cambios
- DS1: Definir y administrar niveles de servicio
- DS5: Garantizar la seguridad de los sistemas
- DS10: Administrar los datos
- ME1: Monitorear el desempeño de TI
- ME2: Monitorear y evaluar el control interno

2.3.2.1 Proceso PO1: Definición de un plan estratégico de tecnología de TI

Tabla 3: Modelos de madurez, Proceso PO1

Dominio: Planeación y Organización					
Proceso: PO1 – Definición de un plan estratégico de tecnología de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La alta gerencia desconoce la necesidad de planeación estratégica?		√		
	¿La alta gerencia apoya el plan estratégico?		√		
	¿Existe una estructura de planeación?		√		
	¿La planeación apoya a las metas?		√		
	¿Se desconoce la existencia de planeación?			√	
1	¿La planificación estratégica es conocida por la gerencia TI?		√		
	¿La planificación estratégica se elabora por un requisito comercial específico?			√	
	¿La planificación de la empresa es discutida ocasionalmente en las reuniones de administración?		√		
	¿La posición de riesgo estratégica está identificada informalmente en base a los proyectos?		√		
	¿La planificación estratégica evoluciona constantemente de acuerdo a las necesidades de la empresa?		√		
2	¿El plan estratégico está entendido sustancialmente por la gerencia?	√			
	¿La planificación estratégica se comparte ocasionalmente con la gerencia de ventas?	√			
	¿El plan estratégico ocurre en respuesta a las demandas administrativas?		√		
	¿Hay procesos para identificar actualizaciones del plan?		√		

	¿Dentro de la empresa los procesos de planificación estratégica son claros y concisos?		√		
3	¿Están definidas las políticas que define cuando y como se realiza la planificación estratégica?		√		
	¿La planificación estratégica involucra a todo el personal?		√		
	¿Existe algún procedimiento para examinar el proceso en una base regular?			√	
	¿La estrategia global TI incluye una definición global de riesgos?		√		
	¿Las estrategias de los recursos financieros incluyen a todos los ámbitos de la empresa?			√	
4	¿La planificación estratégica tiene la supervisión de la dirección?		√		
	¿La planificación estratégica está definida con mayores responsabilidades niveladas?		√		
	¿La planificación estratégica establece las prácticas estándar y sus excepciones son notadas por la dirección?		√		
	¿Existe un proceso bien definido para equilibrar los recursos necesarios para el desarrollo y funcionamiento de la empresa?		√		
	¿Existe una función de administración definida con mayores responsabilidades niveladas?		√		
5	¿El plan estratégico está considerado dentro de los objetivos comerciales de la empresa?	√			
	¿Existe una función de la planificación estratégica que está integrada con la planificación comercial?			√	
	¿El plan estratégico está diseñado para ser implementado a largo plazo?			√	

	¿El plan estratégico es versátil?			√	
	¿El plan estratégico está diseñado respetando las normas que rigen la empresa?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso PO1:

- Administración del valor de TI
- Alineación de TI con el negocio
- Evaluación del desempeño y la capacidad actual
- Plan estratégico de TI
- Planes tácticos de TI
- Administración del portafolio de TI[32]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso PO1 ascienda a un grado de madurez tres, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Se debe definir un plan estratégico.
- Se debe definir un proceso para identificar actualizaciones en el plan estratégico de la compañía.
- Se debe definir una política de cómo y cuándo se va a realizar la planeación estratégica de TI, esta planeación debe ser conocida por todo el equipo de trabajo y se debe garantizar que sea factible y estructurado.
- Realizar un inventario de las soluciones tecnológicas y la infraestructura actual de la organización.
- En la estrategia general de TI, se debe incluir una definición de los riesgos a los que está expuesta la organización.
- La planeación estratégica de TI se debe discutir en reuniones de la dirección del negocio.

[32] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 30

2.3.2.2 Proceso PO3: Determinar la dirección tecnológica

Tabla 4: Modelos de madurez, Proceso PO3

Dominio: Planeación y Organización					
Proceso: PO3 – Determinar la dirección tecnológica					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa pone interés en planear la infraestructura tecnológica?	√			
	¿Existe un plan de infraestructura?		√		
	¿Hay experiencia y conocimiento para realizar un plan de infraestructura documentado y formal?		√		
	¿Existe personal capacitado en su organización que tenga las habilidades y conocimientos para realizar un plan de infraestructura?		√		
	¿Se entiende la importancia de planear un cambio para focalizar correctamente los recursos?		√		
1	¿Los directivos reconocen la necesidad de un plan pero no lo tienen aún?	√			
	¿El desarrollo de tecnología está muy limitado?		√		
	¿Los directivos enfocan su atención en la necesidad de realizar planeación?	√			
	¿La dirección de la tecnología del negocio está a cargo de vendedores o personas incorrectas?			√	
	¿La comunicación es inconsistente sobre el impacto en cambios de tecnología?	√			
2	¿Se comunica la necesidad y la importancia de realizar un plan tecnológico?		√		
	¿La planeación se enfoca en solucionar problemas técnicos en vez de cumplir las necesidades del negocio?			√	

	¿La evaluación de cambios tecnológicos está a cargo de diferentes individuos que siguen procesos similares?		√		
	¿Existe un entrenamiento formal y comunicación de los roles y responsabilidades?		√		
	¿Se reconoce en su organización que están apareciendo técnicas y estándares comunes para el desarrollo de la infraestructura?		√		
3	¿Los directivos conocen sobre el plan de infraestructura tecnológica?	√			
	¿El plan estratégico de TI está alineado con el plan de infraestructura tecnológica?			√	
	¿Se creó un plan de infraestructura tecnológica definido, documentado y bien comunicado pero inconsistente para su aplicación?		√		
	¿Los empleados y directivos entienden a donde se dirige la organización considerando riesgos y alineado con el plan estratégico?		√		
	¿Se seleccionan los mejores vendedores considerando su experiencia y conocimiento para la compra de tecnología?		√		
4	¿El plan estratégico de infraestructura tecnológica fue creado por gente con experiencia?		√		
	¿Se capacita de manera formal y especializada a los nuevos empleados para que conozcan el plan estratégico de la empresa?			√	
	¿Se tiene en cuenta el impacto del cambio de tecnología?		√		
	¿Se anticipa a los problemas y se asignan responsables para cumplir y actualizar el plan de infraestructura tecnológica?			√	

	¿Se introducen las mejores prácticas internas en los procesos?			√	
5	¿Se dirige la empresa utilizando estándares de la industria?		√		
	¿Se administra con alto nivel los impactos que los cambios de tecnología generan?			√	
	¿Se aprueba de manera ejecutiva el cambio de tecnología?			√	
	¿Está formalizada la participación en estándares?			√	
	¿Se utiliza de manera exhaustiva las mejores prácticas de la industria?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso PO3:

- Planeación de la dirección tecnológica
- Plan de infraestructura tecnológica
- Monitoreo de tendencias y regulaciones futuras
- Estándares tecnológicos
- Consejo de arquitectura de TI[33]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso PO3 ascienda a un grado de madurez dos, como estrategia a corto plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Se debe difundir la necesidad de la planeación tecnológica para que haya un enfoque en generar soluciones técnicas a problemas técnicos, en lugar de que se utilice a la tecnología para satisfacer las necesidades del negocio.
- El personal encargado debe aprender sus habilidades sobre planeación tecnológica a través de un aprendizaje y una aplicación repetida de las técnicas.
- Debe existir un entrenamiento formal y comunicación de los roles de todos los empleados y sus responsabilidades.
- Se debe contar con técnicas y estándares comunes para el desarrollo de la infraestructura tecnológica.

[33] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 38

2.3.2.3 Proceso PO4: Definir procesos, organización y relaciones de TI

Tabla 5: Modelos de madurez, Proceso PO4

Dominio: Planeación y Organización					
Proceso: PO4 – Definir procesos, organización y relaciones de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización de TI se centra efectivamente a enfocar el logro de los objetivos del negocio?		√		
1	¿Las actividades y funciones de TI están implementadas, pero son inconsistentes?	√			
	¿Se ha definido una estructura organizacional, roles y responsabilidades que están informalmente asignadas?	√			
	¿La función de TI se considera una función de soporte que no incluye en su totalidad la perspectiva de organización?	√			
2	¿Existe un entendimiento implícito acerca de la necesidad de implementar una organización de TI?		√		
	¿Roles y responsabilidades no están formalizados o no se cumplen?		√		
	¿La función de la TI está organizada para responder tácticamente, pero inconsistentemente?	√			
	¿La necesidad para una organización estructurada y de administración está vilmente comunicada, pero las decisiones que se toman son dependientes del conocimiento y de las herramientas claves de uso individual?			√	
	¿Existen técnicas emergentes comunes para administrar la organización de TI y sus relaciones?		√		
3	¿Se han definido roles y responsabilidades para la organización de la TI y de terceros?		√		
	¿La organización de la TI está desarrollada,			√	

	documentada, comunicada y alineada con la estrategia de TI?				
	¿El diseño organizacional y el control interno del entorno están definidos?		√		
	¿Hay formalización de relaciones con otras partes interesadas?			√	
	¿La organización de TI está funcionalmente completa?		√		
4	¿El personal de la TI tiene la experiencia y formación necesaria para desarrollar un plan de infraestructura de tecnología?		√		
	¿Existe un formal y especializado entrenamiento para la investigación de la tecnología?			√	
	¿La responsabilidad para el desarrollo y mantenimiento de un plan de infraestructura de tecnología podría ser asignada?			√	
	¿La estrategia de los recursos humanos está alineada con la dirección de la tecnología para asegurar que el personal de la TI pueda manejar los cambios de la tecnología?			√	
	¿La dirección de TI está guiada por la industria y estándares internacionales y de desarrollo?			√	
5	¿Existe aprobación ejecutiva formal de un nuevo cambio de reglas tecnológicas?			√	
	¿La entidad tiene un plan de infraestructura robusta que refleje los requerimientos del negocio?			√	
	¿Existe una continua y real mejora de los procesos en el ambiente de trabajo?			√	
	¿Las mejores prácticas de la industria están extensivamente usadas en determinadas reglas de la			√	

	técnica de las TI's?				

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso PO4:

- Marco de trabajo de procesos de TI
- Comité estratégico de TI
- Comité directivo de TI
- Ubicación organizacional de la función de TI
- Estructura organizacional
- Establecimiento de roles y responsabilidades
- Responsabilidad de aseguramiento de calidad de TI
- Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
- Propiedad de datos y sistemas
- Supervisión
- Personal de TI
- Personal clave de TI
- Políticas y procedimientos para personal contratado[34]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso PO4 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Todo el personal de TI debe tener roles formalizados y todos estos roles se deben cumplir.
- La unidad de TI debe organizarse de tal manera que sea capaz de responder de forma táctica a las necesidades de los clientes y los distintos proveedores.
- Conocer responsabilidades del nivel directivo sobre el área de TI.
- Conocer la dirección de la Gerencia y supervisión de TI.
- Se debe revisar que el área de TI se alinee con el negocio y que haya una correcta participación de esta área en los procesos de decisión clave.
- Controlar que se determinen funciones de seguridad, calidad y control interno.

[34] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 42,43

2.3.2.4 Proceso PO9: Evaluar y administrar riesgos de TI

Tabla 6: Modelos de madurez, Proceso PO9

Dominio: Planeación y Organización					
Proceso: PO9 – Evaluar y administrar riesgos de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Se realiza un análisis sobre el riesgo de imposición de contribuciones para procesos y decisiones del negocio?			√	
1	¿La organización considera los impactos de negocio asociados con vulnerabilidades de seguridad y con desarrollo de proyectos inciertos?	√			
	¿El manejo de riesgos se ha visto identificado como relevante para adquirir soluciones de TI y deliberadamente servicios de TI?		√		
	¿La organización sabe de sus responsabilidades tanto legal como contractual y riesgos, considerándolos en una manera ad hoc?	√			
	¿El manejo de TI especifica las responsabilidades para el manejo de riesgos en descripciones de trabajo u otros significados informales?		√		
	¿La especificación de TI relaciona riesgos tales como seguridad e integridad y son ocasionalmente considerados en un proyecto como base principal del mismo?		√		
2	¿Los riesgos de TI relacionados día a día a las diferentes operaciones de la TI son infrecuentemente discutidos en las reuniones de la AG?		√		
	¿Los riesgos consideran que la mitigación o calma es inconsistente dentro del área de TI?		√		
	¿Existe un deseo emergente de entender que los	√			

	riesgos de TI son importantes y necesarios para ser considerados?				
	¿Hay algún acercamiento al riesgo de distribución de contribuciones existentes, dentro del área de TI?			√	
3	¿El área de TI define generalmente procedimientos o descripciones de trabajo gestionando con la Gerencia de TI?		√		
	¿La distribución de contribuciones en las diferentes operaciones de TI depende mediáticamente de un manejo creciente, por lo que esta tiene una gran importancia dentro de la agenda de trabajo?		√		
	¿El riesgo de distribución de contribuciones sigue un proceso definido que es documentado y reconocido por todo el personal a través del entrenamiento?			√	
	¿Las decisiones que se toman a consideración por la AG son salidas efectivas a una posible crisis dentro de la TI?			√	
	¿La metodología es convincente y segura?			√	
4	¿Todos los proyectos que fueron cubiertos o están en operación son examinados sobre una base de riesgos?		√		
	¿El manejo de la política de una organización grande define cuándo y cómo debe conducirse los riesgos de distribución de contribuciones?			√	
	¿La distribución de contribuciones de riesgo es un procedimiento y excepciones a seguir por la AG?			√	
	¿El manejo de los riegos de TI está definido en función con el nivel de responsabilidad de la AG?			√	
	¿La AG es notificada de los cambios en el entorno de la TI lo cual puede significativamente afectar al escenario de riegos?			√	
5	¿La AG es capaz de monitorear la posición de riesgo y			√	

	adoptar una decisión acertada que sea acogida por el personal de la TI?				
	¿El manejo efectivo de una base de datos de riegos está debidamente establecido?			√	
	¿La distribución de contribuciones habría de desarrollar una organización la cual siga regularmente el buen manejo de su estructura?			√	
	¿El análisis y reporte de riegos son altamente automatizados?			√	
	¿El manejo de riegos es verdaderamente aceptable y extensible para los miembros de la USI?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso PO9:

- Marco de trabajo de administración de riesgos
- Establecimiento del contexto del riesgo
- Identificación de eventos
- Evaluación de riesgos de TI
- Respuesta a los riesgos
- Mantenimiento y monitoreo de un plan de riesgos[35]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso PO9 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Los riesgos de TI relacionados día a día a las diferentes operaciones de TI se deben discutir siempre en las reuniones con la Gerencia General.
- Debe existir un enfoque de evolución de riesgos en desarrollo y debe ser implementado en discreción del gerente de TI.
- Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos.
- Debe haber un entrenamiento al personal para que entiendan que los riesgos de TI son importantes y necesarios y deben ser siempre considerados.

[35] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 64

2.3.2.5 Proceso AI5: Instalar y acreditar sistemas

Tabla 7: Modelos de madurez, Proceso AI5

Dominio: Adquisición e Implementación					
Proceso: AI5 – Instalar y acreditar sistemas					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa tiene un proceso formal de instalación de nuevas tecnologías tanto de hardware como de software?		√		
	¿La empresa posee un proceso formal que verifica que la solución sea adecuada y esté alineada con los objetivos de TI?		√		
	¿El personal reconoce la necesidad de verificar si las soluciones que se dan encajan con el propósito deseado?	√			
1	¿La empresa reconoce la necesidad de verificar y confirmar que las soluciones que se implementen contribuyen al propósito deseado?	√			
	¿La empresa realiza pruebas para algunos proyectos?	√			
	¿La empresa depende de iniciativas del equipo del proyecto para realizar las pruebas?		√		
	¿Los resultados que obtiene la empresa al realizar las pruebas usualmente varían?		√		
	¿La empresa tiene una acreditación formal y estar fuera de línea es esporádico o inexistente?		√		
2	¿La empresa tiene alguna consistencia entre la comprobación y la acreditación?		√		
	¿La empresa basa sus pruebas en metodologías?	√			
	¿Existe normalmente una ausencia de comprobación de la integración?		√		
	¿Existe cierto proceso de la aprobación informal, no		√		

	necesariamente basado en un criterio regularizado?				
	¿Existe una acreditación formal y estar fuera de línea es aplicado incoherentemente?		√		
3	¿Está implementada una metodología formal relacionada con la instalación, migración, conversión y existe una aceptación?			√	
	¿Existe la habilidad de mantener un cumplimiento en la administración?		√		
	¿Se encuentran integrados y de alguna forma automatizados los procesos de Instalación y acreditación de TI dentro del ciclo de vida del sistema?			√	
	¿Los entrenamientos, pruebas y la transición entre el estado de producción y acreditación varían de los procesos definidos, y se basan en decisiones individuales?		√		
	¿Es inconsistente la calidad de los sistemas que ingresan a la etapa de producción, generando así problemas de post-implementación?		√		
4	¿Los procesos se encuentran formalizados y desarrollados para encontrarse bien organizados y ser prácticos, con ambientes de prueba y procesos de acreditación definidos?			√	
	¿La evaluación para alcanzar los requerimientos de usuario está estandarizada y puede ser medida?			√	
	¿La calidad de los sistemas que ingresan a la etapa de producción es satisfactoria para la administración?			√	
	¿Se emplean evaluaciones post-implementación ni revisiones continuas de calidad?			√	
	¿El sistema de pruebas refleja de forma adecuada el ambiente real?			√	

5	¿Los procesos de instalación y acreditación se encuentran refinados a un nivel de las mejores prácticas, basados en una continua mejora y refinamiento?			√	
	¿Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y automatizados?			√	
	¿Se disponen de ambientes de prueba bien desarrollados y los procesos de registro de problemas y fallas aseguran una transición de eficiencia y efectividad hacia el ambiente de producción?			√	
	¿La acreditación se da con una mínima necesidad de reformularla y los problemas post-implementación son correcciones menores?			√	
	¿Las revisiones de post-implementación son estandarizadas y son retroalimentadas hacia los procesos para asegurar una continua mejora en cuanto a la calidad?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso AI5:

- Control de adquisición
- Administración de contratos con proveedores
- Selección de proveedores
- Adquisición de recursos de TI[36]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso AI5 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Se debe crear una conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI.
- Las políticas y procedimientos de la empresa, se deben integrar parcialmente con el proceso general de adquisición de la organización del negocio.
- Los distintos procesos de adquisición se deben utilizar en proyectos menores y deben ser bastante visibles para luego implementarlos en cada proyecto de la empresa.
- Se deben determinar responsabilidades para administrar correctamente la adquisición y contratos de TI según la experiencia de cada persona a cargo.
- La empresa debe reconocer la importancia de administrar sus proveedores y las distintas relaciones entre ellos.

[36] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 90

2.3.2.6 Proceso AI6: Administrar cambios

Tabla 8: Modelos de madurez, Proceso AI6

Dominio: Adquisición e Implementación					
Proceso: AI6 – Administrar cambios					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Existe un proceso definido de administración de cambio y estos cambios se pueden realizar virtualmente sin control?			√	
1	¿Existen políticas de administración y control de cambios tecnológicos en la organización?	√			
	¿Se sigue algún proceso consistente a seguir para el control de cambios tecnológicos?		√		
	¿Cambia continuamente el proceso de cambios tecnológicos en la organización?	√			
	¿Se requiere de autorización superior para ejecutar cambios de tecnología?	√			
	¿Cuándo un cambio de tecnología se ejecuta en la organización, es necesario documentar el mismo?			√	
2	¿Existe un proceso formal definido para el proceso de administración y control de los cambios?			√	
	De existir este proceso, ¿está estructurado formalmente?			√	
	¿Considera que la documentación de configuración es precisa y consistente?			√	
	¿Considera que las tareas de planeamiento e impacto son prioritarias a los cambios?			√	
	¿Existe frecuentemente un re-doble de trabajo, en tareas ya efectuadas?	√			
	¿Existe un proceso formalmente definido para la administración de cambios?			√	

3	¿El proceso de administración de cambios incluye priorización, categorización, control de contingencias, autorización de cambios y administración de lanzamientos?			√	
	¿Considera que el proceso de administración de cambios es siempre práctico y aplicable?			√	
	¿Ocurren cambios sin autorización ocasionalmente?	√			
	¿Existe un análisis operacional del impacto que causan los cambios tecnología en el negocio?			√	
4	¿Se sigue de forma consistente el proceso de administración de cambios, confía que en el mismo no hay excepciones?			√	
	¿El proceso de administración de cambios mantiene procesos y controles manuales para asegurar calidad?			√	
	¿Están sujetos los cambios a reducir la posibilidad de problemas post-producción, a través de las tareas de planificación e impacto?			√	
	¿Considera que las tareas planeamiento e impacto son prioritarias a los cambios?			√	
	¿El monitoreo de cambios es un proceso formal dentro de los documentos de administración de cambios?			√	
5	¿Se actualiza regularmente el proceso de administración de cambios?			√	
	¿El proceso de administración de cambios cambia de acuerdo a la línea de las "mejores prácticas"?			√	
	¿La información de configuración se encuentra implementada en una aplicación para controlar la misma?			√	
	¿El monitoreo de la configuración y de la administración de lanzamientos, incluye herramientas		√		

	para la detección de software sin licencia o sin autorización?				
	¿La administración de cambios tecnológicos está integrada a los cambios del negocio?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso AI6:

- Estándares y procedimientos para cambios
- Evaluación de impacto, priorización y autorización
- Cambios de emergencia
- Seguimiento y reporte del estatus de cambio
- Cierre y documentación del cambio[37]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso AI6 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Se debe lograr que el proceso de administración de cambio no sea un proceso informal para evitar que el proceso no sea estructurado, rudimentario y propenso a errores.
- Se debe hacer que la exactitud de la documentación de la configuración sea consistente y no sea de planeación limitada.
- La evolución del impacto de los cambios de TI se debe dar previamente al cambio.

[37] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 94

2.3.2.7 Proceso DS1: Definir y administrar niveles de servicio

Tabla 9: Modelos de madurez, Proceso DS1

Dominio: Entrega y Soporte					
Proceso: DS1 – Definir y administrar niveles de servicio					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La administración ha reconocido la necesidad de un proceso para definir niveles de servicio?		√		
	¿Están asignados responsables cuando existen problemas en los procesos?		√		
	¿Están asignadas las responsabilidades para la administración de servicios?		√		
	¿Están definidos los niveles de servicio?		√		
	¿La administración conoce sobre las obligaciones y responsabilidades que tiene en cuanto a niveles de servicio?		√		
1	¿Existe conciencia de la necesidad de administrar niveles de servicio?		√		
	¿El proceso para la administración de Niveles de Servicio es informal?	√			
	¿Está definida informalmente la rendición de cuentas del desempeño de monitoreo?			√	
	¿Las mediciones del desempeño son cualitativas?			√	
	¿El reporte del desempeño es frecuente?			√	
2	¿Existen acuerdos celebrados sobre el nivel de servicio?			√	
	¿El reporte de nivel de servicio es relevante y completo?			√	
	¿El reporte de nivel de servicio depende de las habilidades de los administradores individuales?			√	
	¿Se debería nombrar un coordinador de nivel de	√			

	servicio?				
	¿El proceso de cumplimiento del acuerdo de nivel de servicio es voluntario?			√	
3	¿Están bien definidas las responsabilidades de la administración de nivel de servicio?			√	
	¿El proceso de desarrollo de los acuerdos de nivel de servicio está establecido con puntos de verificación?			√	
	¿Están definidos con los usuarios los criterios de niveles de servicios?			√	
	¿Están identificadas las carencias de nivel de servicio?			√	
	¿El nivel de servicio puede resolver las necesidades específicas de la organización?			√	
4	¿La satisfacción del cliente se determina de manera rutinaria?			√	
	¿Las medidas de desempeño reflejan las metas de TI?			√	
	¿Están estandarizados los criterios de medición de los niveles de servicio?			√	
	¿Se realiza un análisis de causas originarias?			√	
	¿Están entendidos con claridad los riesgos operativos?		√		
5	¿Los niveles de servicio son reevaluados constantemente?			√	
	¿Todos los procesos de nivel de servicio están sujetos a procesos de mejoramiento?			√	
	¿Un criterio para definir niveles de servicio es basarse en la criticidad del negocio?			√	
	¿Los niveles de satisfacción del cliente son monitoreados?			√	
	¿Los niveles de servicio esperados son evaluados			√	

	contra las normas de la industria?				

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso DS1:

- Marco de trabajo de la administración de los niveles de servicio
- Definición de servicios
- Acuerdos de niveles de servicio
- Acuerdos de niveles de operación
- Monitoreo y reporte del cumplimiento de los niveles de servicio
- Revisión de los acuerdos de niveles de servicio y los contratos[38]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso DS1 ascienda a un grado de madurez uno, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Debe existir la necesidad de administrar los niveles de servicio aun si el proceso sea informal y reactivo.
- Se debe definir la responsabilidad y la rendición de cuentas sobre la definición y la administración de servicios.
- Se debe definir medidas para medir el desempeño, pero en este nivel de madurez aun se las define de forma imprecisa.
- Existe una notificación pero aun es informal, infrecuente e inconsistente.

[38] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 102

2.3.2.8 Proceso DS5: Garantizar la seguridad de los sistemas

Tabla 10: Modelos de madurez, Proceso DS5

Dominio: Entrega y Soporte					
Proceso: DS5 – Garantizar la seguridad de los sistemas					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa reconoce la necesidad de seguridad para el área de TI?	√			
	¿Se asignan responsabilidades para encargarse de la seguridad?		√		
	¿Existe la implementación de medidas que soporten la administración de TI?		√		
	¿La empresa posee un proceso de administración para la seguridad de TI?		√		
	¿Existen procesos de reportes y soluciones para problemas de seguridad en TI?			√	
1	¿La empresa reconoce la necesidad de la seguridad en TI?	√			
	¿La seguridad es administrada según criterios del individuo responsable?	√			
	¿Las responsabilidades para la administración de seguridad en TI son confusas?			√	
	¿Hay una persona responsable para la administración de problemas de seguridad?			√	
	¿Las soluciones para problemas de seguridad son previsibles?		√		
2	¿Las responsabilidades de seguridad de TI son asignadas a un coordinador de seguridad sin autoridad de gerencia?			√	
	¿El reporte de la seguridad es pertinente?			√	

	¿El conocimiento acerca de la seguridad es fragmentado y limitado?		√		
	¿La información de la seguridad es generada pero no analizada?		√		
	¿Las políticas de seguridad están siendo desarrolladas pero se utilizan técnicas y herramientas inadecuadas?		√		
3	¿La Empresa promueve el conocimiento acerca de la seguridad?		√		
	¿Los informes de la seguridad se han formalizado y se han estandarizado?			√	
	¿Los procesos de seguridad de TI están definidos y es complemento de la estructura de políticas y procedimientos de seguridad?		√		
	¿Las responsabilidades para la seguridad de TI son asignadas pero no consistentemente cumplidas?	√			
	¿Existe un plan de seguridad conduciendo a análisis de riesgo y soluciones de seguridad?			√	
4	¿Las responsabilidades para la seguridad de TI son claramente asignadas, administradas y ejecutadas?			√	
	¿Las políticas y prácticas de seguridad son completas, con específicas y bases de seguridad?			√	
	¿Los informes sobre la seguridad de TI se han convertido en una obligación?			√	
	¿La Empresa establece la certificación de seguridad en el personal?			√	
	¿Los procesos de la seguridad de TI son coordinados con la función global de seguridad de la empresa?			√	
5	¿Los requerimientos de seguridad de TI están claramente definidos, optimizados e incluidos en el plan de seguridad?			√	
	¿Los incidentes de seguridad de TI son tratados			√	

	puntualmente con los procedimientos formalizados soportados por herramientas automatizadas?				
	¿Los procesos de seguridad y tecnologías están integrados totalmente a la empresa?			√	
	¿Las funciones de seguridad se integran con las aplicaciones en la etapa de diseño?			√	
	¿Las pruebas de intrusión, análisis de causalidad y la identificación de riesgos no están perfectamente implementadas?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso DS5:

- Administración de la seguridad de TI
- Plan de seguridad de TI
- Administración de identidad
- Administración de cuentas del usuario
- Pruebas, vigilancia y monitoreo de la seguridad
- Definición de incidente de seguridad
- Protección de la tecnología de seguridad
- Administración de llaves criptográficas
- Prevención, detección y corrección de software malicioso
- Seguridad de red
- Intercambio de datos sensitivos[39]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso DS5 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Las responsabilidades y la rendición de cuentas sobre la seguridad se deben asignar a un coordinador de seguridad de TI, aunque en este nivel de madurez, la autoridad del coordinador es limitada.
- Se debe analizar la información que producen los sistemas relevantes al aspecto de seguridad.
- En este nivel de madurez se empieza a desarrollar las políticas de seguridad.
- Se debe ver a la seguridad de TI primordialmente como responsabilidad y disciplina de TI.

[39] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 102

2.3.2.9 Proceso DS10: Administrar los datos

Tabla 11: Modelos de madurez, Proceso DS10

Dominio: Entrega y Soporte					
Proceso: DS10 – Administrar los datos					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Hay conciencia de la necesidad de administrar problemas e incidentes?	√			
	¿El proceso de resolución de problemas es informal?	√			
	¿Los usuarios y el personal de TI resuelven los problemas de manera individual?		√		
	¿Los problemas se resuelven caso por caso?		√		
	¿Existen procesos para el manejo de incidentes?		√		
1	¿La organización ha reconocido que hay una necesidad de resolver problemas y de evaluar los incidentes?	√			
	¿Las personas con conocimientos clave proveen alguna asistencia con los problemas relacionados con su área de experiencia y responsabilidad?	√			
	¿La información es compartida con otros y las soluciones varían de una persona de soporte a otra?	√			
	¿Con medidas equivocadas se da la creación de más problemas y la pérdida de tiempo productivo, mientras se buscan las respuestas?		√		
	¿La administración cambia frecuentemente el enfoque y la dirección de las operaciones y el personal de soporte técnico?		√		
2	¿Hay una amplia conciencia de la necesidad de administrar los problemas e incidentes relacionados con TI?	√			

	¿El proceso de resolución ha evolucionado hasta un grado en que unas pocas personas claves son responsables de administrar los problemas e incidentes que ocurren?			√	
	¿La información es compartida entre el personal; sin embargo, el proceso sigue sin estructuración, es informal y mayormente reactivo?	√			
	¿El nivel de servicio para la comunidad de usuarios varía y es obstaculizado por insuficientes conocimientos estructurados disponibles para quienes resuelven los problemas?		√		
	¿El reporte de la administración de incidentes y el análisis de la creación de problemas es limitado e informal?	√			
3	¿La necesidad de un sistema efectivo de administración de problemas es aceptada y evidenciada por presupuestos para la contratación de personal?			√	
	¿Los procesos de resolución, escalamiento y resolución de problemas han sido estandarizados, pero no son sofisticados?			√	
	¿Los usuarios han recibido comunicaciones claras sobre dónde y cómo reportar sobre problemas e incidentes?			√	
	¿El registro y rastreo de problemas y sus resoluciones es fragmentado dentro del equipo de respuestas, usando las herramientas disponibles sin centralización o análisis?			√	
	¿Es probable que las desviaciones de las normas o estándares establecidos pasen desapercibidas?	√			

4	¿El proceso de administración de problemas es entendido en todos los niveles dentro de la organización?			√	
	¿Las responsabilidades son claras y establecidas?		√		
	¿Los métodos y procedimientos están documentados, comunicados y medidos por efectividad?			√	
	¿La mayoría de los problemas e incidentes están identificados, registrados, reportados y analizados en busca de constante mejoramiento y son reportados a las partes interesadas?			√	
	¿La capacidad de responder a los incidentes es probada periódicamente?			√	
5	¿El proceso de administración de problemas ha evolucionado en un proceso que mira hacia adelante y es proactivo, contribuyendo a los objetivos de TI?			√	
	¿Los problemas son anticipados y pueden incluso ser prevenidos?			√	
	¿El conocimiento es mantenido, a través de contactos regulares con vendedores y expertos, respecto de patrones de problemas e incidentes pasados y futuros?			√	
	¿El registro, reporte y análisis de problemas y resoluciones es automatizado y está totalmente integrada con la administración de configuración de datos?			√	
	¿La mayoría de los sistemas han sido equipados con mecanismos automáticos de detección y de advertencia, que son constantemente rastreados y evaluados?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso DS10:

- Administración de la seguridad de TI
- Plan de seguridad de TI
- Administración de identidad
- Administración de cuentas del usuario
- Pruebas, vigilancia y monitoreo de la seguridad
- Definición de incidente de seguridad
- Protección de la tecnología de seguridad
- Administración de llaves criptográficas
- Prevención, detección y corrección de software malicioso
- Seguridad de red
- Intercambio de datos sensitivos[40]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso DS10 ascienda a un grado de madurez dos, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Asignar un responsable para que monitoree los problemas.
- Establecer procesos estructurados y formales para el escalamiento y resolución de problemas.
- Contar con suficientes pistas de auditoría de problemas y soluciones, los cuales están integrados con la administración de datos de configuración, permitiendo la oportuna resolución de los problemas reportados.
- Generar reportes de incidentes que estén integrados con la administración de datos de configuración, para que se pueda resolver los problemas reportados.
- Emplear mecanismos automáticos de advertencia y detección, para su evaluación continua.
- Disponer de información de los problemas pasados y futuros, para optimizar la solución de problemas internos de la empresa.

[40] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 112

2.3.2.10 Proceso ME1: Monitorear el desempeño de TI

Tabla 12: Modelos de madurez, Proceso ME1

Dominio: Monitoreo y Evaluación					
Proceso: ME1 – Monitorear el desempeño de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización cuenta con un proceso de monitoreo?		√		
	¿El área de TI desarrolla independientemente un monitoreo de proyectos o procesos?		√		
	¿Se reconoce la necesidad de objetivos de procesos claramente entendibles?	√			
1	¿Se reconoce la necesidad de colectar y determinar información acerca de procesos de monitoreo?	√			
	¿Se han identificado procesos determinados y una colección estándar?			√	
	¿Se implementa un monitoreo constante solamente cuando un incidente causa alguna perdida a la organización?			√	
	¿Se implementa el monitoreo para los procesos de TI y tan solo para servicios de información de otros departamentos?			√	
	¿La definición del proceso y el monitoreo se ajustan a las necesidades de los servicios de información?			√	
2	¿Han sido identificadas algunos parámetros para monitorear?			√	
	¿Se ha adoptado una colección de métodos y técnicas, pero no por toda la organización?			√	
	¿La planeación y administración es realizada por la experiencia de individuos claves?		√		

	¿Algunas herramientas son implementadas y usadas pero se limita el uso por falta de experiencia en el manejo?		√		
	¿La función de servicios de información es manejada como un centro que genera costos y no beneficia a la organización?			√	
3	¿La administración ha institucionalizado y comunicado los estándares para monitorear procesos?			√	
	¿Un programa de educación y entrenamiento para monitorear ha sido implementado?			√	
	¿Han sido implementadas herramientas para monitorear el nivel de servicio y procesos de TI?			√	
	¿Han sido definidos parámetros para medir la contribución del nivel de servicio en la organización?			√	
	¿Han sido implementados los parámetros para medir la satisfacción del cliente y del nivel de servicio en las entidades?		√		
4	¿La gerencia define tolerancias en las cuales los procesos deben operar?			√	
	¿Lineamientos base de resultados de monitoreo son estandarizados y normalizados?			√	
	¿Existe integración de las métricas entre proyectos TI y procesos?			√	
	¿Se define un marco para identificar estrategias orientadas a procesos como KGIs, KPIs, y CSFs para realizar mediciones?			√	
	¿Se ejecutan criterios de aprendizaje tales como financieros, operacionales, de consumidores y organizacional?			√	
5	¿Se mejora el proceso para actualizar el monitoreo de estándares, políticas y mejores prácticas en la organización?			√	

	¿Todos los procesos de monitoreo son optimizados y soportan objetivos globales de la organización?			√	
	¿KGIs, KPIs, y CSFs son usados continuamente para realizar mediciones y se alinean con el trabajo estratégico?			√	
	¿Procesos de monitoreo y rediseños en movimiento son consistentes con planes ya desarrollados de mejoramiento?			√	
	¿Bancos de prueba contra la industria y competidores claves se formalizan y comparan?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso ME1:

- Enfoque del monitoreo
- Definición y recolección de datos de monitoreo
- Método de monitoreo
- Evaluación del desempeño
- Reportes al Consejo Directivo y a Ejecutivos
- Acciones correctivas[41]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso ME1 ascienda a un grado de madurez uno, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

- Implementar un proceso de monitoreo y evaluación de desempeño de TI
- La empresa debe contar con reportes útiles, oportunos y precisos.
- Se debe definir estándares de recolección y evaluación de acuerdo a las necesidades de los proyectos y procesos específicos de TI.
- Definir reportes e indicadores de desempeño.
- Realizar evaluaciones de satisfacción al usuario, para tener un mejoramiento continuo del servicio brindado.
- Estandarizar y normalizar el proceso de reportes.

[41] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 154

2.3.2.11 Proceso ME2: Monitorear y evaluar el control interno

Tabla 13: Modelos de madurez, Proceso ME2

Dominio: Monitoreo y Evaluación					
Proceso: ME2 – Monitorear y evaluar el control interno de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización posee procedimientos para monitorear la efectividad de los controles internos?			√	
	¿Los métodos de reporte de control interno de administración están presentes en su organización?			√	
	¿Hay una ausencia general de conciencia de la seguridad operativa?	√			
	¿La administración y los empleados tienen conciencia de los controles internos?		√		
	¿Hay una ausencia general del aseguramiento de control interno de TI?		√		
1	¿Existe un compromiso de parte de la administración para la seguridad operativa regular?			√	
	¿Se aplica ad hoc en la experiencia individual en determinar la adecuación de control interno?			√	
	¿La administración de TI ha asignado formalmente la responsabilidad de monitorear la efectividad de los controles Internos?			√	
	¿Las evaluaciones de control interno de TI son realizadas como parte de auditorías financieras tradicionales?			√	
	¿Existe un monitoreo adecuado dentro de la empresa?		√		
2	¿La organización usa reportes informales de control para iniciar iniciativas de acción correctiva?			√	
	¿Los procesos de planificación y administración están definidos?			√	

	¿La evaluación depende de los conjuntos de habilidades de las personas clave?			√	
	¿La organización tiene una mayor conciencia del monitoreo de control interno?			√	
	¿La administración ha comenzado a establecer métricas básicas?			√	
3	¿La administración soporta y ha institucionalizado un monitoreo de control interno?			√	
	¿Se han desarrollado políticas y procedimientos para evaluar y reportar sobre las actividades de control interno?			√	
	¿No se ha establecido una base de conocimientos de métrica para información histórica sobre el monitoreo de control interno?			√	
	¿No se ha implementado un programa de educación y entrenamiento para el monitoreo de control interno?			√	
	¿Se han establecidos revisiones periódicas para el monitoreo del control Interno?			√	
4	¿La administración ha establecido Benchmarking y metas cuantitativas para los procesos de revisión del control interno?			√	
	¿La organización estableció niveles de tolerancia para el proceso de monitoreo de control interno?			√	
	¿Están incorporadas herramientas integradas y cada vez más automatizadas en los procesos de revisión del control interno?			√	
	¿Los riesgos específicos del proceso y las políticas de mitigación están definidos para toda la función de servicios de Información?			√	
	¿Está establecida una función formal de control interno de TI con profesionales?			√	

5	¿La administración ha establecido un programa de mejoramiento continuo a través de toda la organización?			√	
	¿La organización usa herramientas avanzadas que son integradas y actualizadas?			√	
	¿Está formalizada la participación de los conocimientos?			√	
	¿Están implementados programas formales de entrenamiento específicos para la función de los servicios de información?			√	
	¿Los marcos de control de TI están integrados con marcos y metodologías a nivel de toda la organización?			√	

Fuente: realizado en base a las tablas propuestas por la Ing. Nidia Guayaquil en base al Manual Cobit 4.1 en español

Cobit 4.1 establece los siguientes objetivos de control para el proceso ME2:

- Monitorización del marco de trabajo de Control Interno
- Revisiones de Auditoría
- Excepciones de control
- Control de auto evaluación
- Aseguramiento del Control Interno
- Control Interno para terceros
- Acciones correctivas[42]

Siendo el objetivo primordial de un modelo de madurez el ascender a un grado de madurez superior, para que el proceso ME2 ascienda a un grado de madurez uno, como estrategia a corto y largo plazo y conforme lo establece Cobit 4.1, se recomienda lo siguiente:

[42] Adler, Mark. Manual Cobit 4.1 en español. Rolling Meadows, IL, IT Governance Institute, 2007, 158

- Implementar procedimientos para monitorear la efectividad de los controles internos.
- Asignar de manera formal las tareas para monitorear la efectividad de los controles internos y evaluarlos en base a la necesidad de los servicios de información.
- Establecer responsabilidades para el control interno.
- Realizar monitoreo permanente de control interno.
- Establecer programas de mejora continua dentro de la empresa.

2.4 Análisis de Resultados

2.4.1 Resultados del análisis realizado con Cobit 4.1

En base a las Matrices de Madurez aplicadas a los procesos seleccionados de Cobit 4.1 se ha encontrado lo siguiente:

2.4.1.1 Dominio Planeación y Organización

Nivel de Madurez: Uno

Conclusiones:

- Es necesario implementar un plan estratégico, en el que se defina un proceso que permita identificar y realizar actualizaciones del mismo. Se debe implementar una política de cómo y cuándo se va a realizar la planeación estratégica de TI, la que debe ser conocida por todo el equipo de trabajo y se debe garantizar que sea el plan que se realice sea factible y estructurado. La planeación estratégica debe ser discutida en reuniones con la Dirección y se debe contar con técnicas y estándares comunes para el desarrollo de la infraestructura tecnológica. La estrategia general de TI, debe incluir una definición de los riesgos a los que está expuesta la organización.
- Es importante que se difunda la necesidad de la planeación tecnológica para que exista un enfoque en generar soluciones a problemas técnicos que permitan satisfacer las necesidades del negocio Los riesgos de TI relacionados al día a día a las diferentes operaciones de TI, deben ser discutidos siempre en las reuniones con la Gerencia General; además debe existir un enfoque de evolución de riesgos en desarrollo y debe ser implementado en discreción del gerente de TI. El personal encargado de realizar la planeación, debe potenciar sus habilidades sobre planeación tecnológica, a través de un aprendizaje y una aplicación repetida de las técnicas, así como un entrenamiento formal. Debe también existir comunicación de los roles de todos los empleados y sus responsabilidades, especialmente de los empleados de la unidad de TI, quienes deben tener roles formalizados, los cuales deben ser cumplidos a cabalidad..

- La unidad de TI debe organizarse de tal manera, que sea capaz de responder de forma táctica y oportuna a las necesidades de los clientes y los distintos proveedores, la organización de la unidad de TI debe ser estructurada de tal manera, que las decisiones dependan del conocimiento y las habilidades de los individuos clave; debe contar con técnicas emergentes comunes para administrar la organización de TI y sus relaciones con los demás departamentos, además debe haber un deseo emergente del personal de entender que los riesgos de TI son importantes y necesarios y deben ser siempre considerados.

2.4.1.2 Dominio Adquisición e Implementación

Nivel de Madurez: Uno

Conclusiones:

- Se debe crear una conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Estas políticas y procedimientos deben ser integrados parcialmente con el proceso general de adquisición de la organización del negocio, los que deben ser utilizados en proyectos menores y deben ser usados como base para luego implementarlos en cada proyecto que maneje la empresa. Se debe lograr que el proceso de administración de cambio no sea un proceso informal para evitar que el proceso no sea estructurado, rudimentario y propenso a errores, la empresa debe reconocer la importancia de administrar sus proveedores y las distintas relaciones entre ellos.
- Se deben determinar responsabilidades para administrar correctamente la adquisición y contratos de TI según la experiencia de cada persona a cargo y que la exactitud de la documentación de la configuración sea consistente y no sea de planeación limitada, de tal manera que la evolución del impacto de los cambios de TI sean previos al cambio.

2.4.1.3 Dominio Entrega y Soporte

Nivel de Madurez: Uno

Conclusiones:

- La empresa debe desarrollar las políticas de seguridad, pues es necesario que exista la necesidad de administrar los niveles de servicio aun si el proceso sea informal y reactivo. Para la definición y administración de los servicios, se debe definir la responsabilidad y la rendición de cuentas, las que se deben asignar a un coordinador de seguridad de TI, aunque en este nivel de madurez, la autoridad del coordinador es limitada. Se deben definir medidas para medir el desempeño, para poder analizar la información que producen los sistemas relevantes al aspecto de seguridad. La seguridad del departamento de TI se debe ver primordialmente como una responsabilidad y disciplina del área de TI.
- Se deben generar reportes de incidentes que estén integrados con la administración de datos de configuración, para que se pueda resolver los problemas reportados, además de emplear mecanismos automáticos de advertencia y detección, para su evaluación continua, se debe contar con suficientes pistas de auditoría de problemas y soluciones, los cuales deben ser integrados con la administración de datos de configuración, permitiendo de esta manera, la oportuna resolución de los problemas reportados, también hay que contar con información de los problemas pasados que ha enfrentado la empresa y posibles problemas futuros, para optimizar la solución de problemas internos de la organización.

2.4.1.4 Dominio Monitoreo y Evaluación

Nivel de Madurez: Cero

Conclusiones:

- La empresa debe contar con reportes útiles, oportunos y precisos, los que se deben estandarizar y normalizar; además se debe definir estándares de recolección y evaluación de acuerdo a las necesidades de los proyectos y procesos específicos de TI, para tener un mejoramiento continuo de los distintos servicios que brinda la empresa, se debe realizar evaluaciones de satisfacción al usuario, a más de establecer programas de mejora continua dentro de la empresa.
- La compañía debe implementar procedimientos para monitorear la efectividad de los controles internos, establecer responsabilidades para el control interno, realizar un monitoreo permanente de control interno y asignar de manera formal las tareas para monitorear la efectividad de los controles internos y evaluarlos en base a la necesidad de los servicios de información.

CAPITULO TRES

APLICACIÓN DE LA NORMA OCTAVE-S EN LA EMPRESA

3.1 Identificación de los Riesgos Informáticos

Para realizar correctamente la evaluación OCTAVE-S dentro de la empresa Pirámide Digital Cía. Ltda. es necesario definir un equipo de trabajo interdisciplinario, el que será responsable de llevar a cabo varias actividades, se debe contar con personal del área de Altos Directivos, área Operativa y área de Personal en General; esto ayudará a tener una perspectiva más amplia de la empresa a nivel tecnológico y organizacional.

3.1.1 Roles y Responsabilidades del Equipo de Análisis

- Trabajar con los directivos para definir el alcance de la evaluación.
- Programación de actividades OCTAVE-S.
- Realización de las actividades de evaluación.
- Recopilar, analizar y mantener los datos de evaluación durante la evaluación.
- Logística de coordinación para la evaluación.[43]

3.1.2 Habilidades del Equipo de Análisis

- Capacidad para gestionar las reuniones de grupo.
- Buenas habilidades de comunicación.
- Buenas habilidades analíticas.
- Conocimiento del entorno de negocio de la organización.
- Conocimiento del entorno de la organización de tecnología de la información y la forma en que el personal de las empresas legítimamente utiliza la tecnología de la información en la organización.[44]

[43] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 8

[44] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 9

3.1.3 Selección de Altos Directivos

Los Altos Directivos que se van a seleccionar para la evaluación, deben tener la capacidad y conocimientos necesarios para identificar correctamente los activos de información más importantes dentro de la empresa, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

3.1.3.1 Perfil de Altos Directivos

- Estar familiarizado con los tipos de activos de información utilizados en la empresa.
- Ser capaz de destinar el tiempo requerido para las evaluaciones.
- Tener conocimiento de los procesos clave que maneja la empresa para la ejecución normal de sus actividades y tareas.
- Tener autoridad de seleccionar y autorizar el tiempo para los Directivos de áreas operativas.
- Haber estado en su cargo por lo menos un año.[45]

3.1.4 Selección de los Directivos de Áreas Operativas

Los Directivos de Áreas Operativas deben estar asociados a la operación, mantenimiento y desarrollo de la infraestructura computacional de la organización; son requeridos para identificar los activos de información que posee la empresa, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

3.1.4.1 Perfil de los Directivos de Áreas Operativas

- Amplio conocimiento con los tipos de activos de información que utiliza la empresa.
- Conocer cómo los activos de información son utilizados.
- Conocimiento de los activos críticos de la organización.
- Tener la autoridad de seleccionar y autorizar el tiempo necesario para el personal en general.
- Haber estado en su cargo por lo menos dos años.[46]

[45] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 11

[46] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 13

3.1.5 Selección del Personal en General

Se necesita con personal que se encargue de identificar los activos de información que se consideren importantes para la organización, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

3.1.5.1 Perfil del Personal en General

- Conocer los tipos de activos de información usados en la organización y cómo son utilizados.
- Conocimiento respecto al tema de riesgo e impacto hacia los activos críticos de las tecnologías de información.
- Conocimiento de estándares de mitigación, medición y controles de riesgo asociados a TI.
- Haber estado en su cargo por lo menos tres años.[47]

3.1.6 Selección del Equipo de Trabajo para la empresa Pirámide Digital Cía. Ltda.

Una vez realizada la selección entre el personal más idóneo para que forme parte del equipo de trabajo que realizará la evaluación en la organización, se han seleccionado a los siguientes profesionales:

3.1.6.1 Altos Directivos

- Ing. Mario Morillo Gerente de Tecnología

3.1.6.2 Directivos de Áreas Operativas

- Eco. Olga Obando Gerente de Consultoría

3.1.6.3 Personal en General

- Sr. Guillermo Obando Asistente de Tecnología

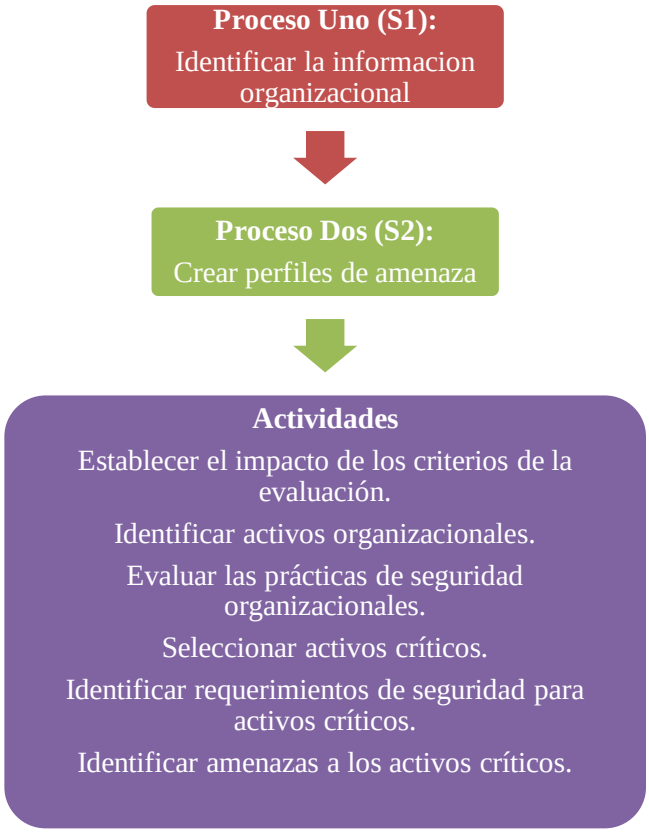
[47] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 15

3.2 Fase Uno: Construcción del perfil de amenaza basado en los activos

En esta fase, se realiza una evaluación de los aspectos organizacionales donde el equipo de trabajo define el impacto de los criterios de la evaluación que se utilizará para realizar una evaluación de riesgos, también se identificarán cuales son los activos organizacionales y se evaluarán las prácticas de seguridad que se practican actualmente en la empresa.

En esta fase, se identifican dos procesos:

Figura 8: Método Octave-S, Fase Uno



Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 6

3.2.1 Proceso S1: Identificar la información organizacional

3.2.1.1 Establecer el impacto de los criterios de la evaluación

Tabla 14: Hoja de Trabajo. Impacto de los criterios de la evaluación: Reputación y Confianza del Cliente

Reputación/Confianza del Cliente			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Reputación	La reputación de la empresa se afecta en un mínimo porcentaje, poco o nada de esfuerzo o gasto es necesario para recuperarse si se presenta la situación de pérdida de confianza del cliente.	La reputación de la empresa se daña, y esfuerzo y un poco de gasto económico se requiere para recuperarse.	La reputación de la empresa está irremediablemente destruida o dañada.
Otro:			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 34-35

Tabla 15: Hoja de Trabajo. Impacto de los criterios de la evaluación: Finanzas

Finanzas			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Costos operativos	Aumento de menos de *2%* anual en costos operativos	Gastos anuales de costos operativos aumentan del *2%* al *10%*	Anualmente los costos operativos aumentan el *10%*
Pérdida de ingresos	Menos de *5%* de pérdida de ingresos anuales	De *5%* al *12%* de pérdida de ingresos anuales	Mayor del *12%* en pérdida de ingresos anuales
Pérdida financiera	Pérdida financiera de menos de *$5000*	Pérdida financiera de *$5000* a *$15000*	Pérdida financiera mayor a *$15000*
Otro:			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 36-37

Tabla 16: Hoja de Trabajo. Impacto de los criterios de la evaluación: Productividad

Productividad			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Horarios del personal	El horario del personal se incrementó menos del *5%* en *28* día(s)	El horario del personal se incrementó entre el *5%* al *20%* en *28* día(s)	El horario del personal se incrementó en más de un *20%* en *28* día(s)
Otro:			
Otro:			
Otro:			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 38-39

Tabla 17: Hoja de Trabajo. Impacto de los criterios de la evaluación: Seguridad/Salud

Seguridad/Salud			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Vida	No hay pérdida o amenaza significativa en la vida del personal	La vida de los miembros del personal se ven amenazadas, pero se recuperarán después de recibir tratamiento médico.	Pérdida de vidas de miembros del personal
Salud	Degradación mínima, inmediatamente tratable de la salud de los miembros del personal con un tiempo de recuperación dentro de cuatro días	Discapacidad temporal o recuperable de la salud de miembros del personal	Deterioro permanente de la salud de miembros del personal
Seguridad	Seguridad cuestionada	Seguridad afectada	Seguridad violada
Otro:			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 40-41

Tabla 18: Hoja de Trabajo. Impacto de los criterios de la evaluación: Multas/Sanciones Legales

Multas/Sanciones Legales			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Multas	Multas inferiores *$1000* son recaudadas	Multas entre *$1000* y *$5000* son recaudadas	Multas mayores a *$5000* son recaudadas
Demandas	Demandas no frívolas de menos de *$1000* son presentadas en contra de la organización	Demandas no frívolas entre *$1000* y *$5000* son presentadas en contra de la organización	Demandas no frívolas mayores a *$5000* son presentadas en contra de la organización
Investigaciones	No hay preguntas formuladas por el gobierno u otras organizaciones de investigación	El gobierno u otras organizaciones de investigación requieren información o records de la empresa	El gobierno u otras organizaciones de investigación inician una investigación de alto perfil y en profundidad de las prácticas de la organización
Otro:			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 42-43

Mediante el uso de las Hojas de Trabajo: Impacto de los criterios de la evaluación, se definió los rangos de posibles impactos que se pueden presentar en la organización.

Se cuenta con suficiente información sobre la naturaleza de impactos causados por problemas comunes y situaciones de emergencia, y utilizó esta información como base para el establecimiento de medidas (alto, medio, bajo) a través de múltiples áreas de impacto.

Pirámide Digital Cía. Ltda. cuenta con un presupuesto el cual incluye un margen del 2% para cambios inesperados en los costos de operación y un margen del 5% para cambios inesperados en los ingresos totales.

Se determinó que cualquier pérdida de vida o daños permanentes a los empleados en las instalaciones de la organización se considera inaceptable. Estos artículos se incorporaron en los criterios de evaluación.

3.2.1.2 Identificar activos organizacionales

Tabla 19: Hoja de Trabajo. Identificación de activos organizacionales: Información, Sistemas y Aplicaciones

Información, Sistemas y Aplicaciones			
Sistema ¿Qué sistemas la gente en su organización necesita para realizar su trabajo?	**Información** ¿Qué información la gente en su organización necesita para realizar su trabajo?	**Aplicaciones y Servicios** ¿Qué aplicaciones y servicios la gente en su organización necesita para realizar su trabajo?	**Otros Activos** ¿Qué otros activos están relacionados directamente con estos activos?
Computadoras personales	• *Propuestas* • *Pagos* • *Presupuestos*	• *email* • *SugarCRM* • *Real VNC* • *Acceso a Internet*	• *Periféricos*
Servidor de correo electrónico	• *Información de correos* • *Información de clientes*	• *Acceso a Internet*	• *Computadoras personales*
Servidor Web (Portal de Gerencia)	• *Información de la empresa* • *Información de cursos gerenciales* • *Información de clientes* • *Presentaciones, Videos, Documentos Gerenciales*	• *Acceso a Internet*	• *Computadoras personales*
SugarCRM	• *Automatización de fuerza de ventas* • *Campañas de marketing*	• *Acceso a Internet*	• *Computadoras personales*

	• *Atención al cliente* • *Presentación de informes*		
Real VNC	• *Acceso y control a servidores*	• *Acceso a Internet*	• *Computadoras personales*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 46-47

Tabla 20: Hoja de Trabajo. Identificación de activos organizacionales: Gente

Gente			
Gente *¿Qué personas tienen una habilidad o conocimiento especial que es vital para su organización y puede ser muy difícil de reemplazar?*	**Habilidades y Conocimiento** *¿Cuáles son sus habilidades o conocimientos?*	**Sistemas Relacionados** *¿Qué sistemas utilizan estas personas?*	**Activos Relacionados** *¿Qué otros activos usan estas personas (Ejemplo: información, servicios o aplicaciones)*
Ing. Pablo Páez, PhD	• *Conocimiento del funcionamiento de los sistemas de la empresa.* • *Contacto con clientes importantes.* • *Representante de partners en el Ecuador.* • *Elaboración de propuestas.* • *Trainer de la mayoría de los cursos que ofrece la empresa.* • *Negociación con clientes.*	• *Computadora personal* • *SugarCRM* • *Portal de Gerencia*	
Eco. Olga Obando, PhD	• *Conocimiento del portafolio de servicios que ofrece Pirámide Digital.* • *Facilidad para*	• *Computadora personal.* • *SugarCRM.* • *Portal de Gerencia*	

	identificar las necesidades especificas del cliente y proponer soluciones a través de los distintos servicios que ofrece la empresa. • *Elaboración, presentación y discusión de propuestas.* • *Análisis costo-beneficio de las propuestas.* • *Negociación con los clientes.* • *Coordinación del equipo de consultores en los trabajos de campo.* • *Coordinación y dirección del personal.* • *Directora de proyectos de la empresa.*		

Ing. Mario Murillo	• *Conocimiento de redes.* • *Conocimiento de bases de datos.* • *Manejo de SugarCRM.* • *Soporte, actualización y mantenimiento de todos los servidores propios y servidores alojados en Estados Unidos.*	• *Computadora personal* • *SugarCRM.* • *Servidor web* • *Servidor de correo*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 48-49

El equipo de trabajo utilizó su conocimiento de los sistemas que Pirámide Digital Cía. Ltda. como punto de partida para identificar los activos de la empresa.

Al utilizar las Hojas de Trabajo: Identificación de activos organizacionales, para identificar los activos, los miembros del equipo observaron la cantidad de información que reside en los servidores de Pirámide Digital. La información de sus clientes, que se regula en términos de privacidad y seguridad, se puede encontrar en varias formas, incluyendo tanto electrónico como archivos de papel. Se observó que las computadoras personales son comunes a todos los sistemas y funcionan como un conducto para toda la información electrónica importante.

Fue más difícil identificar a las personas claves relacionadas con el patrimonio de la empresa, ya que cada miembro del personal tiene un papel importante en Pirámide Digital sin embargo, se decidió que sólo las personas con habilidades especiales o conocimientos que no podían sustituirse fácilmente se deben documentar como activos durante la evaluación.

En el caso de Pirámide Digital se identificó que la Eco. Olga Obando por tener conocimiento y realizar la mayor parte de actividades relacionadas con el cliente, el manejo de relaciones, elaboración de propuestas y coordinación del equipo de consultores es indispensable para las operaciones del día a día.

De igual manera, tanto Pablo Páez PhD como el Ing. Mario Morillo también se identificaron como personas importantes relacionados con los activos de la empresa y sería muy difícil encontrar y contratar dos personas que asuman estas responsabilidades sin que afecte o interrumpa las operaciones de Pirámide Digital.

3.2.1.3 Evaluar las prácticas de seguridad organizacionales

Tabla 21: Hoja de Trabajo. Prácticas de seguridad: Seguridad, Concientización y Entrenamiento

Seguridad, Concientización y Entrenamiento				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Los miembros del personal comprendan sus roles de seguridad y responsabilidades. Esto está documentado y verificado.	Si Algo (No) No se sabe	• *Los miembros del personal tienen tareas definidas.* • *Miembros del personal siguen la buena práctica de no divulgar información confidencial y definición de contraseñas.*	• *Falta de capacitación para el personal de TI.* • *Personal no entiende todos los riesgos de seguridad.* • *Poco conocimiento de roles y acciones de seguridad.* • *Personal utiliza una sola contraseña para acceder a todas las*	Rojo (Amarillo) Verde No aplica
Hay suficiente experiencia interna para todas las versiones servicios, mecanismos y tecnologías. Esto está documentado y verificado.	Si Algo (No) No se sabe			
Existe una conciencia de seguridad, capacitación y recordatorios	Si Algo (No) No se sabe			

periódicos, los que se proporcionan para todo el personal. El entendimiento del personal está documentado y se verifica periódicamente.			*aplicaciones* • *No existe documentación formal de roles de seguridad.* • *No hay documentación de servicios mecanismos y tecnología.* • *No hay roles y responsabilidades definidas.*	
Los miembros del personal siguen buenas prácticas como: • Asegurar información de la que son responsables • No divulgar información confidencial a otros • Tener capacidad suficiente para utilizar la información tecnología de hardware y software • Uso de buenas prácticas para definir contraseñas • Entender y	Si (Algo) No No se sabe			

seguir las políticas de seguridad y los reglamentos • Reconocer y reportar incidentes				

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 52-53

Tabla 22: Hoja de Trabajo. Prácticas de seguridad: Estrategia de Seguridad

Estrategia de Seguridad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Las estrategias comerciales de la organización incorporan consideraciones de seguridad.	Si (Algo) No No se sabe		• *La actual estrategia de seguridad de la empresa no es efectiva.*	(Rojo) Amarillo Verde No aplica
Las estrategias y políticas de seguridad toman en cuenta las estrategias y objetivos del negocio de la organización.	Si Algo (No) No se sabe		• *La estrategia de seguridad no se encuentra bien documentada y le falta enfoque empresarial. No es proactiva.*	
Las estrategias de seguridad, metas y objetivos son documentados y se revisan de forma rutinaria, se lo actualiza y se comunica a todos.	Si Algo (No) No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 54-55

Tabla 23: Hoja de Trabajo. Prácticas de seguridad: Gestión de la Seguridad

Gestión de la Seguridad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
La Gerencia asigna fondos y recursos suficientes para actividades de información de seguridad.	Si Algo (No) No se sabe	• *El equipo y el personal están de acuerdo en que la evaluación de riesgos es dar un paso en la dirección correcta que beneficiará a la organización*	• *No hay fondos suficientes en el presupuesto para seguridad.* • *Miembros del personal se encuentran satisfechos con el nivel de seguridad actual.* • *No hay roles definidos*	(Rojo) Amarillo Verde No aplica
Los roles y responsabilidades de seguridad se definen para todo el personal de la organización.	Si Algo (No) No se sabe			
Todo el personal en todos los niveles de responsabilidad pone en práctica sus funciones asignadas.	Si Algo (No) No se sabe			
Existen procedimientos documentados para la autorización y supervisión de todo el personal (incluido el				

personal tercerizado) que trabajan con sensible información o que trabajan en lugares donde la información reside.				
Las prácticas de contratación y terminación de personal en la organización se toman en cuenta la seguridad informática.	Si Algo No (No se sabe)			
La organización gestiona los riesgos de seguridad de la información: • Evalúa los riesgos para la seguridad de la información • Toma medidas para mitigar riesgos de seguridad de la información	Si Algo (No) No se sabe			
Gerencia recibe y actúa sobre los informes de rutina relacionados con la seguridad de la	Si Algo No (No se sabe)			

información (por ejemplo, auditorías, registros y evaluaciones de vulnerabilidad).				

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 56-57

Tabla 24: Hoja de Trabajo. Prácticas de seguridad: Políticas de Seguridad y Regulaciones

Políticas de Seguridad y Regulaciones				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
La organización cuenta con un amplio conjunto de políticas actuales que periódicamente son revisadas y actualización.	Si (Algo) No No se sabe	• *Existe una práctica establecida cualquier incidente.*	• *No todo el personal conoce sobre esta práctica.* • *La gente no siempre sigue esta práctica.* • *La práctica de seguridad no se revisa, no está docuementada.*	(Rojo) Amarillo Verde No aplica
Hay un procedimiento documentado de gestión de las políticas de seguridad, que incluye: • Creación • Administración (revisiones periódicas y actualizaciones) • Comunicación	Si (Algo) No No se sabe			

La organización dispone de un procedimiento documentado para evaluar y garantizar el cumplimiento de las políticas de seguridad, leyes y regulaciones aplicables, y requisitos de seguro.	Si Algo (No) No se sabe			
La organización uniformemente refuerza sus políticas de seguridad.	Si Algo (No) No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 58-59

Tabla 25: Hoja de Trabajo. Prácticas de seguridad: Plan de Contingencia/Recuperación de Desastres

Plan de Contingencia/Recuperación de Desastres				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Se ha realizado un análisis de las operaciones, las aplicaciones y los datos críticos.	Si (Algo) No No se sabe		• *No existe un plan de recuperación ante desastres naturales o emergencia* • *No existe plan de continuidad del negocio.* • *No hay un plan de recuperación para sistemas o redes.*	(Rojo) Naranja Verde No aplica
La organización ha documentado, revisado y probado: • Planes de continuidad del negocio y de operación en caso de emergencia • Plan de recuperación de desastres (s)	Si Algo (No) No se sabe			
Los planes de contingencia, recuperación de desastres y de negocios consideran	Si Algo (No) No se sabe			

la continuidad física y electrónica y los requisitos de acceso y controles.				
Todo el personal: • Esta consciente de los planes de recuperación de desastres imprevistos y continuidad del negocio. • Comprende y es capaz de realizar sus responsabilidades.	Si Algo (No) No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 62-63

Tabla 26: Hoja de Trabajo. Prácticas de seguridad: Control de Acceso Físico

Control de Acceso Físico				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Planes de seguridad de las instalaciones y procedimientos para salvaguardar las instalaciones, edificios y cualquier zona restringida y están documentados y probados.	Si Algo (No) No se sabe	• *Existe una política de manejo de visitantes, pero no es propia de la empresa, sino establecida por el edificio donde se encuentra las oficinas de la empresa en Quito.* • *Para el acceso a la sala de servidores se requiere de*	• *La seguridad física se ve afectada debido a que en ocasiones se comparten laptops, se conocen contraseñas de la otra persona y se comparte el espacio en la oficina.*	Rojo (Naranja) Verde No aplica
Hay políticas y procedimientos documentados para la gestión de los visitantes.	Si (Algo) No No se sabe			
Hay políticas y procedimientos documentados para controlar el acceso	Si (Algo) No No se sabe			

físico a las áreas de trabajo y hardware (ordenadores, dispositivos de comunicación, etc.) y soporte de software.		*una tarjeta magnética.* • *Todos los equipos de la oficina necesitan de una clave de acceso.* • *Estaciones de trabajo y servidores están físicamente salvaguarda dos.*		
Las estaciones de trabajo y otros componentes que permiten acceso a información sensible están físicamente salvaguardados para prevenir el acceso no autorizado.	(Si) Algo No No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 64-65

Tabla 27: Hoja de Trabajo. Prácticas de seguridad: Gestión del Sistema y la Red

Gestión del Sistema y la Red				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Existen planes de seguridad para salvaguardar el sistema y las redes.	Si Algo (No) No se sabe	• *Se realizan cambios de contraseña para todos los usuarios cada seis meses.* • *Acceso a servidores y sistemas están protegidos con contraseñas* • *Existen copias de seguridad.* • *Se da mantenimiento a hardware*	• *No existe un plan documentado de seguridad.* • *No todos los sistemas están actualizados* • *No hay planes de control de hardware y software planeados* • *No hay procedimientos formales para cambio de contraseñas*	Rojo (Naranja) Verde No aplica
La información confidencial está protegida en un almacenamiento seguro (por ejemplo, copias de seguridad almacenadas en otro sitio).	(Si) Algo No No se sabe			
La integridad del software instalado es regularmente verificada.	Si (Algo) No No se sabe			

Todos los sistemas están actualizados a la fecha de acuerdo con revisiones, parches y recomendaciones de seguridad.	Si (Algo) No No se sabe	*y software una vez cada año.*	*o manejo de usuarios.*	
Existe un plan documentado y comprobado para la copia de seguridad de los datos de software. Todo el personal entiende sus responsabilidades en virtud de los planes de copia de seguridad.	Si Algo (No) No se sabe			
Todos los cambios de hardware y software son planeados, controlados y documentados.	Si (Algo) No No se sabe			
Los miembros del área de TI siguen procedimientos para cambiar y dar de baja contraseñas, cuentas y privilegios.	Si (Algo) No No se sabe			

Solo los servicios necesarios están corriendo en los sistemas, todos los servicios que no son necesarios han sido eliminados.	Si Algo (No) No se sabe			
Herramientas y mecanismos para el sistema de seguridad y administración de la red que se utilizan, se revisan de manera rutinaria, se actualizan o reemplazan.	Si (Algo) No No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 68-69

Tabla 28: Hoja de Trabajo. Prácticas de seguridad: Monitoreo y Auditoría de la Seguridad de TI

Monitoreo y Auditoría de la Seguridad de TI				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Sistema y red de monitoreo y herramientas de auditoría son habitualmente utilizados por la organización. Actividades inusuales se manejan de acuerdo con las políticas y procedimientos definidos.	Si (Algo) No No se sabe	• *Se realizan monitoreos del sistema.* • *Se monitorea el servidor de seguridad regularmente*	• *No se reporta actividad inusual.* • *No hay políticas definidas.*	Rojo (Naranja) Verde No aplica
Componentes del Firewall y otros componentes de seguridad son auditados periódicamente para	Si (Algo) No No se sabe			

revisar el cumplimiento de políticas.				

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 70-71

Tabla 29: Hoja de Trabajo. Prácticas de seguridad: Manejo de la Vulnerabilidad

Manejo de la Vulnerabilidad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Hay un conjunto de procedimientos documentados para manejo de vulnerabilidades, para: • Seleccionar las herramientas de evaluación de vulnerabilidad, listas de control y secuencias de comandos • Mantenerse al día con la vulnerabilidad conocida, tipos y métodos de	Si Algo (No) No se sabe		• *No hay procedimientos definidos para poder manejar la vulnerabilidad en la organización.*	(Rojo) Naranja Verde No aplica

ataque • Revisar las fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicación • Identificación de los componentes de infraestructura a ser evaluado • Programar evaluaciones de vulnerabilidad • Interpretar y responder a los resultados • Mantener un almacenamiento seguro y la disposición de datos vulnerables				
Se siguen procedimientos de gestión de vulnerabilidades los que son	Si Algo (No) No se sabe			

periódicamente revisados y actualizados.				
Evaluaciones de tecnología vulnerable se realizan en forma periódica, y las vulnerabilidades se abordan cuando se las identifica.	Si Algo (No) No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 74-75

Tabla 30: Hoja de Trabajo. Prácticas de seguridad: Encriptación

Encriptación				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: • Controles apropiados de seguridad se utilizan para proteger información sensible durante el almacenamiento y durante la transmisión (por ejemplo, el cifrado de datos, infraestructura de clave pública, tecnología de red privada virtual).	Si Algo (No) No se sabe	• *Se maneja una red privada virtual.*	• *No se protege información el momento de enviarla vía correo electrónico mediante encriptación.* • *Nunca se ha discutido proteger información mediante encriptación.*	(Rojo) Naranja Verde No aplica

Se utilizan protocolos de cifrado cuando se maneja sistemas, routers y firewalls a distancia.	Si Algo (No) No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 76-77

Tabla 31: Hoja de Trabajo. Prácticas de seguridad: Seguridad de Diseño y Arquitectura

Seguridad de Diseño y Arquitectura				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Arquitectura del sistema y diseño para sistemas nuevos y actualizaciones que incluyen las siguientes consideraciones: • Estrategias de seguridad, políticas y procedimientos • Antecedentes de compromisos de seguridad. • Resultados de las evaluaciones de riesgos de	Si Algo (No) No se sabe	• *Existe el diagrama de arquitectura de red de la empresa*	• *No se ha discutido con el personal sobre seguridad del diseño y la arquitectura*	(Rojo) Naranja Verde No aplica

seguridad.				
La organización tiene diagramas que muestran la seguridad en toda la empresa y la arquitectura de red que están actualizados.	Si Algo No No se sabe			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 78-79

Tabla 32: Hoja de Trabajo. Prácticas de seguridad: Manejo de Incidentes

Manejo de Incidentes				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Existen procedimientos documentados para la identificación, presentación de informes, y procesos para responder a incidentes sospechosos y violaciones.	Si Algo (No) No se sabe		• *No existen procedimientos para presentar informes o procesos para responder a incidentes sospechosos y violaciones.* • *Nunca se ha considerado desarrollar una política para tratar con incidentes sospechosos violaciones o autoridades policiales.* • *No se*	(Rojo) Naranja Verde No aplica
Los procedimientos de manejo de incidentes son periódicamente probados, verificados y actualizados.	Si Algo (No) No se sabe			

Existen políticas y procedimientos documentados para trabajar con autoridades policiales.	Si Algo (No) No se sabe		*reportan incidentes o violaciones.*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 80-81

Se utilizó la Hoja de Trabajo: Prácticas de seguridad para documentar el estado actual y la eficiencia de las prácticas de seguridad de la organización, para esto se discutieron las preguntas presentadas en las hojas de trabajo hasta llegar a un consenso de hasta que extensión cada práctica de seguridad está presente en Pirámide Digital. Durante esta evaluación, se identificaron fortalezas y debilidades relacionadas a cada práctica de seguridad. La mayoría de áreas evaluadas fueron asignadas bajo el estatus rojo o naranja, ninguna área fue asignada con el estatus verde para prácticas de seguridad.

Se notó que algunas prácticas de seguridad se realizaban correctamente en Pirámide Digital, pero la mayoría no se estaban ejecutando correctamente. Las dos prácticas de seguridad que se ejecutan bien en la organización son: protección de la información confidencial en un almacenamiento seguro y todas las estaciones de trabajo y otros componentes que permiten acceso a información sensible están físicamente salvaguardados para prevenir acceso no autorizado.

Al área de seguridad, concientización y entrenamiento se le asignó estatus rojo ya que no existen roles y responsabilidades de seguridad documentados y verificados, no hay capacitación de seguridad periódica para el personal y no se siguen buenas prácticas de seguridad ya que no hay políticas de seguridad y reglamentos definidos.

Al área de estrategias de seguridad se le asignó estatus rojo ya que la actual estrategia comercial de la empresa no es efectiva, no está documentada y no es proactiva y no hay una política de seguridad definida para la organización.

Al área de gestión de la seguridad se le asignó estatus rojo ya que Gerencia no asigna fondos suficientes para que miembros del personal se capaciten en seguridad, no hay roles y responsabilidades definidos de seguridad para el personal, no existen procedimientos documentados para la autorización y supervisión del personal que trabaja con información sensible ni para manejar la contratación y terminación del personal, la organización no gestiona los riesgos de la seguridad de la información.

Al área de políticas de seguridad y regulaciones se le asignó estatus rojo ya la política de manejo de incidentes no es formal y no se encuentra documentada, no existe un procedimiento documentado para evaluar y garantizar el cumplimiento de políticas de seguridad, leyes, regulaciones, etc.

Al área de plan de contingencia y recuperación de desastres se le asignó estatus rojo debido a que actualmente no existe un plan de recuperación ante desastres naturales o emergencias, plan de continuidad del negocio o de recuperación para sistemas o redes.

Al área de control de acceso físico se le asignó estatus naranja ya que existe control de acceso al área de servidores mediante el uso de una tarjeta magnética, todos los equipos están protegidos con una clave de acceso y también se encuentran físicamente salvaguardados sin embargo, la seguridad física se ve afectada debido a que en ocasiones se comparte computadores o se conocen contraseñas de otras personas, además no existe una política de manejo de visitantes propia de la empresa sino que se utiliza la política que maneja el edificio donde se encuentra la oficina de la empresa en Quito.

Al área de gestión del sistema y la red se le asignó estatus naranja ya que se realizan cambios de contraseñas periódicos para todos los usuarios, el acceso a equipos y sistemas está protegido con contraseñas, la empresa cuenta con copias de seguridad almacenadas en otro lugar y se da mantenimiento a hardware y software una vez al año sin embargo, actualmente no existe un plan de seguridad del sistema y la red documentado, no todos los sistemas están actualizados, no hay planes de control de hardware y software ni procedimientos formales para cambio de contraseñas o manejo de usuarios y no se han eliminado los servicios que no se están utilizando.

Al área de monitoreo y auditoría de la seguridad de TI se le asignó estatus naranja ya que se realizan monitoreos del sistema regularmente sin embargo, no se reporta actividades inusuales de acuerdo con políticas y procedimientos definidos.

Al área de manejo de la vulnerabilidad se le asignó estatus rojo ya que no existen procedimientos definidos para ninguno de los niveles de manejo de vulnerabilidades en la organización.

Al área de encriptación se le asignó estatus rojo ya que nunca se ha discutido proteger la información mediante encriptación, no se protege la información el momento de enviarla via correo electrónico mediante encriptación y tampoco se utilizan protocolos de cifrado para manejar sistemas, routers o firewalls a distancia.

Al área de seguridad de diseño y arquitectura se le asignó estatus rojo ya que si bien existe un diagrama de arquitectura de red de la empresa no se ha hecho ninguna consideración para el manejo de seguridad del diseño y arquitectura de red, no existen políticas de seguridad, antecedentes de compromisos de seguridad ni evaluaciones de riesgos de seguridad.

Y finalmente al área de incidentes se le asignó estatus rojo ya que no existen procedimientos para presentar informes o procesos para responder a incidentes sospechosos y violaciones y nunca se ha considerado desarrollar una política para tratar con autoridades policiales.

3.2.2 Proceso S2: Crear perfiles de amenazas

3.2.2.1 Seleccionar Activos Críticos

Tabla 33: Hoja de Trabajo: Selección de Activos Críticos

Selección de Activos Críticos	
Preguntas a considerar: Qué activo tendría un efecto adverso en la organización si: • ¿Es divulgado a personas no autorizadas? • ¿Es modificado sin autorización? • ¿Se pierde o es destruido? • ¿El acceso al activo es interrumpido?	
Activo Crítico	**Notas**
1. Portal de Gerencia (www.elmayorportaldegerencia.com)	*La empresa depende del Portal de Gerencia*
2. Aplicaciones	*El personal utiliza distintas aplicaciones diariamente.*
3. Cliente	*Todo el personal utiliza computadoras personales para tener acceso a la diferente documentación.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 84-85

Se seleccionaron los siguientes activos críticos:

- Portal de Gerencia: Esta fue una selección obvia para el equipo de trabajo, ya que el Portal de Gerencia es central para que se desarrollen las operaciones de Pirámide Digital, ya que desde aquí se maneja la universidad virtual, se almacenan videos, presentaciones, tips, entre otros documentos necesarios para dictar los diferentes cursos que dicta la empresa. Pirámide Digital debe cumplir con regulaciones para proteger la seguridad y privacidad para asegurar esta información.
- Aplicaciones: Se seleccionó a las aplicaciones como activo crítico ya que varias de estas aplicaciones son utilizadas diariamente por el personal ya sea para el monitoreo continuo del estado de los distintos servidores (RealVNC) o para hacer seguimiento a proyectos, clientes, campañas de marketing, etc. (SugarCRM).
- Cliente: El equipo de análisis concluyó que las computadoras personales eran un activo común para todos los sistemas.

Se registraron todas las opciones para los activos críticos en la Hoja de Trabajo: Selección de Activos Críticos. Posteriormente, se decidió que el Activo Crítico a ser evaluado es el Portal de Gerencia, desde este punto en adelante todos los resultados presentados corresponden a dicho activo critico.

3.2.2.2 Identificar requerimientos de seguridad

Tabla 34: Hoja de Trabajo: Información de Activos Críticos

Información de Activos Críticos				
Activo Crítico ¿Cuál es el sistema crítico?	**Justificación de la Selección** ¿Por qué es ese sistema crítico para la organización?	**Descripción del Sistema** ¿Quién usa el sistema? ¿Quién es responsable de este sistema?	**Requerimientos de Seguridad** ¿Cuáles son los requerimientos de seguridad para este sistema?	**Requerimiento de seguridad más importante** ¿Cuál de los requerimientos de seguridad es el más importante para este sistema?
Portal de Gerencia	*El equipo de trabajo definió que el personal es 80% dependiente del Portal de Gerencia ya que ahí se encuentra almacenada toda la información que se utiliza para los distintos cursos que se dictan, redactar propuestas y la universidad virtual.*	*Todo el personal tiene acceso al portal.* *El encargado de realizar mantenimiento del mismo es el departamento de Sistemas de la empresa.*	**Confidencialidad:** Solo personal autorizado puede ver información *del Portal de Gerencia, se debe considerar que persona tiene acceso a qué información.* **Integridad:** Solo personal autorizado puede modificar información *del Portal de Gerencia.* **Disponibilidad:** *El Portal de Gerencia* debe estar disponible para que	Confidencialidad Integridad Disponibilidad Otro

			el personal realice su trabajo. *El acceso a esta información es requerida 24x7x365*. **Otro:**	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 89

Se discutieron cuáles cualidades del activo crítico Portal de Gerencia eran importantes de proteger, esta discusión resultó en la identificación de los requerimientos de seguridad para este activo crítico.

Seleccionar el requerimiento de seguridad más importante fue una decisión sin embargo, después de considerar y analizar las opciones, se decidió que el requerimiento de seguridad más importante es la disponibilidad del Portal de Gerencia, ya que para realizar actividades cotidianas, dictar cursos o realizar propuestas se necesita acceso continuo e inmediato al Portal.

3.2.2.3 Identificar amenazas a los activos críticos

Tabla 35: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red – Perfil básico de riesgo

Actores con acceso a la red – Perfil básico de riesgo						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*						**Actores de amenazas** *¿Qué actores plantean las mayores amenazas para el sistema a través de la red?*
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**		
Portal	Red	Adentro	Accidental	Revelación Modificación Pérdida Interrupción		***Personas que pertenecen a la organización que actúan accidentalmente:*** *Personas que trabajan en la empresa que discuten información "sensible" en áreas públicas.*
		`	Premeditado	Revelación Modificación Pérdida Interrupción		***Personas que pertenecen a la organización que actúan deliberadamente:*** *Personal descontento, o personas que mal utilizan la información alojada en el Portal de Gerencia y no tienen motivos maliciosos.*
		Afuera	Accidental	Revelación Modificación Pérdida Interrupción		***Personas ajenas a la organización que actúan accidentalmente:*** *Algún técnico que haya sido contratado para que arregle alguna falla de hardware.*

	Premeditado	Revelación	***Personas ajenas a la organización que actúan deliberadamente:*** *Terroristas, espías, hackers.*
		Modificación	
		Pérdida	
		Interrupción	

Motivo						**Historia**			
¿Qué tan fuerte es el motivo del actor?			*¿Qué tan confiado está usted de este estimado?*			*¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Alto	**Medio**	**Bajo**	**Muy**	**Algo**	**Nada**		**Muy**	**Algo**	**Nada**
						5 veces en *2* años		*X*	
						2 veces en *2* años		*X*	
						0 veces en *2* años		*X*	
						0 veces en *2* años		*X*	
		X		*X*		*0* veces en *2* años		*X*	
		X		*X*		*0* veces en *2* años		*X*	
		X		*X*		*0* veces en *2* años		*X*	
		X		*X*		*0* veces en *2* años		*X*	
						0 veces en *2* años	*X*		
						0 veces en *2* años	*X*		
						0 veces en *2* años	*X*		
						0 veces en *2* años	*X*		
		X	*X*			*0* veces en *2* años	*X*		
		X	*X*			*0* veces en *2* años	*X*		
		X	*X*			*0* veces en *2* años	*X*		
		X	*X*			*0* veces en *2* años	*X*		

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 94, 96-97

Tabla 36: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red – Áreas de Preocupación

Gente que pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que pertenecen a la organización actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	*Cualquier empleado que sin ser consciente revela datos importantes, claves o datos importantes de la organización.*
De ejemplos de cómo personas que pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	*Cualquier empleado que tenga acceso físico o remoto al servidor donde se aloja el Portal de Gerencia.*
Gente que no pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que no pertenecen a la organización que actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	*Cualquier técnico que tenga acceso físico a los equipos que deliberada o accidentalmente pueda acceder a información confidencial*
De ejemplos de cómo personas que no pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	*Espías o hackers que quieran acceder al portal pueden intentar hackearlo buscando y explorando limitantes en el código o en las máquinas.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 98-99

Tabla 37: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema

Problemas del Sistema – Perfil básico de riesgo						
Amenaza			**Historia**			
¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			*¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
Portal	Defectos de software	Revelación	*0* veces en *2* años		*X*	
		Modificación	*3* veces en *2* años		*X*	
		Pérdida	*0* veces en *2* años		*X*	
		Interrupción	*7* veces en *2* años		*X*	
	El sistema se cae	Revelación	*0* veces en *2* años		*X*	
		Modificación	*2* veces en *2* años		*X*	
		Pérdida	*1* veces en *2* años		*X*	
		Interrupción	*2* veces en *2* años		*X*	
	Defectos de hardware	Revelación	*0* veces en *2* años		*X*	
		Modificación	*2* veces en *2* años		*X*	
		Pérdida	*2* veces en *2* años		*X*	
		Interrupción	*2* veces en *2* años		*X*	
	Código malicioso	Revelación	*0* veces en *2* años		*X*	
		Modificación	*0* veces en *2* años		*X*	
		Pérdida	*0* veces en *2* años		*X*	
		Interrupción	*0* veces en *2* años		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 112

Tabla 38: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Problemas del Sistema – Áreas de Preocupación

Defectos de Software	
De ejemplos de cómo cualquier defecto de software podría ser considerado una amenazar el sistema.	*Cualquier software mal instalado o sin actualizaciones.*
El sistema se cae	
De ejemplos de cómo si el sistema se cae podría ser considerado una amenazar el sistema.	*Sin acceso al sistema, se detiene la operación.*
Defectos de Hardware	
De ejemplos de cómo cualquier defecto de hardware podría ser considerado una amenazar el sistema.	*Al migrar la información a un nuevo servidor, y no está en producción a tiempo.*
Código Malicioso	
De ejemplos de cómo código malicioso de software podría ser considerado una amenazar el sistema.	*Cualquier vulnerabilidad puede ser explotada a través de un virus o cualquier otro tipo de código malicioso.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 115

Tabla 39: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas

Otros Problemas – Perfil básico de riesgo						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Historia** *¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
Portal	Problemas con el suministro de energía	Revelación	*0* veces en *2* años		*X*	
		Modificación	*3* veces en *2* años			*X*
		Pérdida	*3* veces en *2* años			*X*
		Interrupción	*5* veces en *2* años			*X*
	Problemas de telecomunicaciones	Revelación	*0* veces en *2* años		*X*	
		Modificación	*0* veces en *2* años		*X*	
		Pérdida	*2* veces en *2* años			*X*
		Interrupción	*3* veces en *2* años			*X*
	Problemas con sistemas de terceros	Revelación	*0* veces en *2* años		*X*	
		Modificación	*3* veces en *2* años		*X*	
		Pérdida	*2* veces en *2* años		*X*	
		Interrupción	*6* veces en *2* años		*X*	
	Desastres naturales	Revelación	*0* veces en *2* años		*X*	
		Modificación	*0* veces en *2* años		*X*	
		Pérdida	*0* veces en *2* años		*X*	
		Interrupción	*0* veces en *2* años		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 120

Tabla 40: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas– Áreas de Preocupación

Problemas con el suministro de energía	
De ejemplos de cómo cualquier problema con el suministro de energía podría ser considerado una amenazar el sistema.	*Los UPS no subieron correctamente haciendo que los procesos que estaban corriendo se detengan, en varios casos se ha perdido información.*
Problemas de telecomunicaciones	
De ejemplos de cómo cualquier problema de telecomunicaciones podría ser considerado una amenazar el sistema.	*Sin acceso a internet o conexión a la red interna de Pirámide Digital no se puede monitorear el estado del servidor web.*
Problemas con sistemas de terceros	
De ejemplos de cómo cualquier problema con sistemas de terceros podría ser considerado una amenazar el sistema.	*El momento que se instaló Sugar CRM en el servidor web se tuvo problemas y el envío de campañas de marketing se detuvo.*
Desastres naturales	
De ejemplos de algún desastre natural podría ser considerado una amenazar el sistema.	*No se han registrado amenazas al sistema por desastres naturales.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 122

Tabla 41: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas

Otros Problemas – Perfil básico de riesgo						
Amenaza			**Historia**			
¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			*¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
Portal	Personas clave que renuncian	Revelación	*0* veces en *2* años		*X*	
		Modificación	*1* veces en *2* años		*X*	
		Pérdida	*2* veces en *2* años		*X*	
		Interrupción	*2* veces en *2* años		*X*	
	Personas clave permiso temporal	Revelación	*0* veces en *2* años		*X*	
		Modificación	*3* veces en *2* años		*X*	
		Pérdida	*3* veces en *2* años		*X*	
		Interrupción	*4* veces en *2* años		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 134

Tabla 42: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas– Áreas de Preocupación

Personas clave que toman un permiso temporal	
De ejemplos de cómo si una persona clave en la organización toma un permiso temporal podría ser considerado una amenazar el sistema.	*Cuando una persona clave en la organización salió de vacaciones, hubo una interrupción en el Portal de Gerencia.*
Personas clave que salen de la organización permanentemente	
De ejemplos de cómo si una persona clave en la organización se retira de la empresa permanentemente podría ser considerado una amenazar el sistema.	*Cuando renuncio una persona clave en la empresa, quien conocía como administrar un sistema, tomó tiempo en que la persona que lo iba a reemplazar logre poner en funcionamiento dicho sistema.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 136

Se construyó un perfil de riesgo para el activo critico Portal de Gerencia, registrando el perfil en la Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia, las amenazas correspondientes a los Actores Humanos con acceso a la red y físicos no se deben minimizar o despreciar así no se haya detectado mayor amenaza por los actores con acceso a la red en los últimos dos años, se llegó a esta conclusión basado en la experiencia del equipo y los problemas relacionados con la red y la seguridad física.

La mayoría de las amenazas de la categoría de Problemas del Sistema afectaría por lo general sólo la disponibilidad de la información almacenada en el Portal de Gerencia, la excepción es el código malicioso, ya que no se puede conocer el resultado de esta amenaza. Las amenazas de la otra categoría de Otros Problemas también se cree que afecta sólo a la disponibilidad del Portal de Gerencia.

Se identificaron los tipos de personas que pueden ser consideradas actores amenaza, se documentó distintos tipos de actores potenciales, incluyendo hackers, personal descontento y personal de Pirámide Digital que de manera accidental o premeditado puedan poner en riesgo al activo, ya que la empresa no cuenta con un plan para manejar el acceso a la información o violaciones de seguridad confidencial, el equipo estaba preocupado por la amenaza potencial planteada por cualquier técnico que tenga acceso físico a los equipos que deliberada o accidentalmente pueda acceder a información confidencial.

Con la excepción de algún miembro del personal descontento, se determinó que la amenaza que representa cualquier persona que trabaja para la organización es baja; los motivos de personas del exterior para acceder al Portal de Gerencia fueron difíciles de estimar, pero se llego a la conclusión que debido a que la empresa no es muy grande es un objetivo menos atractivo a hackers o espías. Se decidió que los motivos para personas del exterior que pueden amenazar al sistema es bajo.

La amenaza que presenta un defecto de software, hardware, si el sistema se cae o código malicioso ha generado algunos episodios en los últimos dos años causando modificación, perdida e interrupción en el activo.

El riesgo de que un problema con el suministro de energía, de telecomunicaciones, sistemas de tercero o desastres naturales resultó difícil de estimar y el equipo no se encontraba muy seguro de estos datos, especialmente para estimar la frecuencia de modificación, perdida e interrupción debido a problemas con el suministro de energía y la perdida y interrupción debido a problemas de telecomunicaciones ya que resultó difícil recordar todos los episodios que han sucedido en los últimos dos años.

Otra área de preocupación que puede convertirse en una amenaza al sistema es que si algún miembro del personal que se considera clave en la organización pide un permiso temporal o renuncia se considera como una amenaza al sistema, ya que toma tiempo hacer que otra persona asuma esas responsabilidades haciendo difícil buscar un reemplazo adecuado, esta conclusión la confirma los datos recolectados por el equipo de análisis ya que en dos años han ocurrido casos en que se ha perdido, modificado e interrumpido el activo.

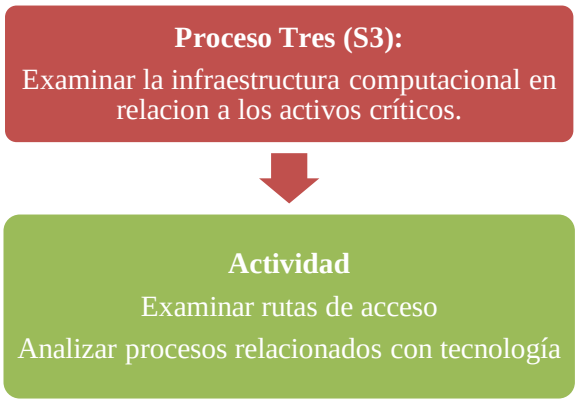
3.3 Fase Dos: Identificar vulnerabilidades de la infraestructura

En esta fase, el equipo de trabajo conduce una revisión de alto nivel de la infraestructura computacional, debe enfocarse en la seguridad, y se debe analizar cómo la gente utiliza la infraestructura computacional para acceder a los activos críticos, y conociendo quién es responsable de configurar y dar mantenimiento a dichos activos críticos.

El equipo de trabajo examina hasta qué punto cada parte responsable realiza con seguridad sus prácticas y procesos de TI.

En esta fase se identifica un proceso:

Figura 9: Método Octave-S, Fase Dos



Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 6

3.3.1 Proceso S3: Examinar la infraestructura computacional en relación a los activos críticos

3.3.1.1 Examinar rutas de acceso

Tabla 43: Hoja de Trabajo: Rutas de acceso

Sistema de interés	
Portal de Gerencia	
Puntos de Acceso	
Sistema de Interés	**Puntos de Acceso Intermedios**
Sistema de Interés *¿Cuál de las siguientes clases de componentes son parte del sistema de interés?*	**Puntos de Acceso Intermedios** *¿Cuál de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones desde el sistema de interés hacia la gente?* *¿Cuál de las siguientes clases de componentes podría servir como un punto de acceso intermedio?*
Servidores Redes Internas Estaciones de trabajo Otros	Red Interna Red externa Otros

Puntos de Acceso		
Acceso al Sistema por Individuos	**Ubicación de donde se almacenan los datos**	**Otros Sistemas o Componentes**
Acceso al Sistema por Individuos *¿De cuál de las siguientes clases de componentes puede la gente (por ejemplo, los usuarios, los atacantes) acceder al sistema de interés?* *Considere puntos de acceso internos y externos a la red de la organización*	**Ubicación de donde se almacenan los datos** *¿En qué clase de componente esta la información del sistema de interés almacenada por motivos de respaldo?*	**Otros Sistemas o Componentes** *¿Cuál otro sistema accede a información del sistema de interés?*
Estaciones de Trabajo Laptops PDAs/Componentes Wireless Estaciones de Trabajo fuera de la oficina Otros	Dispositivos de almacenamiento de respaldos locales Otros	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 140-141

Se utilizó la Hoja de Trabajo: Rutas de acceso, para revisar cómo la gente accede al activo crítico Portal de Gerencia y se identificaron clases de componentes clave que eran parte o se relacionaban con el Portal. Esta actividad incluyó examinar puntos de acceso al Portal de Gerencia y se determinó que el personal usualmente utilizaba estaciones de trabajo, laptops, PDAs y estaciones de trabajo fuera de la oficina para acceder al Portal, se determinó que los puntos de acceso intermedio incluían redes internas y externas y que se contaba con dispositivos de almacenamiento de respaldos locales.

3.3.1.2 Analizar procesos relacionados con tecnología

Tabla 44: Hoja de Trabajo: Evaluación de la infraestructura

Clase *¿Cuál clase de componente está relacionado con uno o más de los activos críticos?*	**Activo Crítico** *¿Cuál activo critico está relacionado con cada clase?*			**Responsabilidad** *¿Quién es responsable de mantener y asegurar cada clase de cada componente?*
	Portal	**Aplicaciones**	**Cliente**	
Servidores				
Servidor web	*X*	*X*	*X*	*Área de Tecnología*
Red interna				
Todos	*X*	*X*	*X*	*Área de Tecnología*
Estaciones de trabajo				
Administrador	*X*	*X*		*Área de Tecnología*
Usuarios	*X*	*X*		*Área de Tecnología*
Laptops				
Administrador	*X*	*X*		*Área de Tecnología*
Usuarios	*X*	*X*		*Área de Tecnología*
Visitantes	*X*			*Área de Tecnología*
PDAs/Componentes Wireless				
Personal	*X*			*Área de Tecnología*
Visitantes	*X*			*Área de Tecnología*

Dispositivos de Almacenamiento				
Respaldo local	*X*	*X*		*Área de Tecnología*
Respaldo off-site	*X*	*X*		*No seguro*
Red Externa				
Todos	*X*			*Desconocido*
Estaciones de trabajo fuera de la oficina				
Administrador	*X*			*Individual*
Usuarios	*X*			*Individual*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 144-147

Para poder realizar esta actividad, se asumió un punto de vista de la infraestructura para analizar la información utilizando la Hoja de Trabajo: Evaluación de la infraestructura, durante este análisis se documentaron las clases de componentes y se analizó cuál activo crítico estaba relacionado a cada clase, también se determino quién era responsable de mantener y asegurar cada clase de componente.

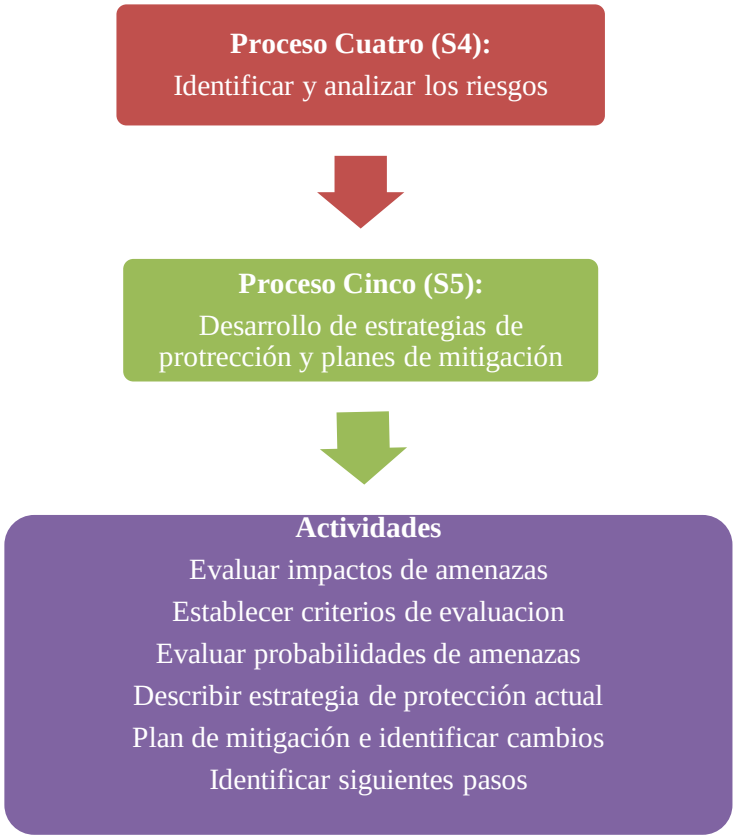
El personal de Pirámide Digital a través del Área de Tecnología da mantenimiento a la mayoría de las clases de componentes, excepto cuando se accede al Portal a través de estaciones de trabajo fuera de la oficina.

3.4 Fase Tres: Desarrollo de planes y estrategias de seguridad

En esta fase, el equipo de trabajo identifica los riesgos s los que los activos críticos de la empresa están expuestos y decide qué hacer con ellos, se basan en un análisis de la información recogida, con esta información el equipo de trabajo desarrolla una estrategia de protección para la organización y planes de mitigación para enfrentar los riesgos de los activos críticos.

En esta fase se identifican dos procesos:

Figura 10: Método Octave-S, Fase Tres



Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 7

3.4.1 Proceso S4: Identificar y analizar los riesgos

3.4.1.1 Evaluar el impacto de las amenazas

Tabla 45: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red. Impacto

Actores con acceso a la red – Impacto											
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*					**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
Portal	Red	Adentro	Accidental	Revelación	*M*	*B*	*A*	*B*	*A*	-
				Modificación	M	B	A	B	A	-
				Pérdida	A	M	A	B	A	-
				Interrupción	A	M	A	B	A	-
			Premeditado	Revelación	M	M	A	B	A	-
				Modificación	M	M	A	B	A	-
				Pérdida	M	M	A	B	A	-
				Interrupción	M	M	A	B	A	-
		Afuera	Accidental	Revelación	M	M	A	B	M	-
				Modificación	M	B	A	B	M	-
				Pérdida	M	M	A	M	M	-
				Interrupción	M	M	M	M	M	-

	Premeditado	Revelación	M	M	A	M	A	-
		Modificación	M	A	A	M	A	-
		Pérdida	M	A	A	M	A	-
		Interrupción	M	A	A	M	A	-

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 94, 118

Tabla 46: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema. Impacto

Problemas del Sistema – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
Portal	Defectos de software	Revelación	*M*	*M*	*A*	*B*	*M*	-
		Modificación	*A*	*M*	*A*	*B*	*A*	-
		Pérdida	*A*	*A*	*A*	*B*	*A*	-
		Interrupción	*A*	*A*	*A*	*M*	*A*	-
	El sistema se cae	Revelación	*M*	*M*	*M*	*B*	*M*	-
		Modificación	*M*	*B*	*M*	*B*	*A*	-
		Pérdida	*A*	*A*	*A*	*B*	*A*	-
		Interrupción	*A*	*A*	*A*	*B*	*A*	-
	Defectos de hardware	Revelación	*M*	*B*	*A*	*B*	*M*	-
		Modificación	*B*	*B*	*A*	*M*	*M*	-
		Pérdida	*A*	*A*	*A*	*M*	*A*	-
		Interrupción	*A*	*A*	*A*	*M*	*A*	-
	Código malicioso	Revelación	*A*	*A*	*A*	*A*	*A*	-
		Modificación	*A*	*A*	*A*	*A*	*A*	-

	Pérdida	*A*	*A*	*A*	*A*	*A*	-
	Interrupción	*A*	*A*	*A*	*A*	*A*	-

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 120

Tabla 47: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Impacto

Otros Problemas – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
Portal	Problemas con el suministro de energía	Revelación	*M*	*M*	*B*	*M*	*B*	-
		Modificación	*M*	*M*	*M*	*M*	*A*	-
		Pérdida	*M*	*M*	*A*	*M*	*A*	-
		Interrupción	*M*	*M*	*A*	*M*	*A*	-
	` Problemas de telecomunicaciones	Revelación	*M*	*M*	*B*	*M*	*B*	-
		Modificación	*M*	*M*	*M*	*M*	*A*	-
		Pérdida	*M*	*M*	*A*	*M*	*A*	-
		Interrupción	*M*	*M*	*A*	*M*	*A*	-
	Problemas con sistemas de terceros	Revelación	*A*	*A*	*B*	*M*	*B*	-
		Modificación	*M*	*M*	*M*	*M*	*A*	-
		Pérdida	*M*	*M*	*A*	*M*	*A*	-
		Interrupción	*M*	*M*	*A*	*M*	*A*	-
	Desastres naturales	Revelación	*A*	*A*	*B*	*M*	*B*	-
		Modificación	*M*	*M*	*M*	*M*	*A*	-

	Pérdida	*M*	*M*	*A*	*M*	*A*	-
	Interrupción	*M*	*M*	*A*	*M*	*A*	-

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 127

Tabla 48: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Impacto

Otros Problemas – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
Portal	Personas clave que tienen permiso temp.	Revelación	*A*	*M*	*M*	*B*	*M*	-
		Modificación	*A*	*M*	*A*	*B*	*A*	-
		Pérdida	*A*	*M*	*A*	*B*	*A*	-
		Interrupción	*A*	*B*	*A*	*B*	*A*	-
	Personas clave que renuncian	Revelación	*A*	*M*	*A*	*B*	*A*	-
		Modificación	*A*	*M*	*A*	*M*	*A*	-
		Pérdida	*A*	*M*	*A*	*M*	*A*	-
		Interrupción	*A*	*M*	*A*	*M*	*A*	-

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 132

La Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Impacto sirvió para evaluar los impactos de las amenazas en la organización, se revisó cada área de interés y discutieron distintos tipos de acciones específicas que habría que adoptar para hacer frente a una amenaza, proporcionando una base para estimar el nivel real de impacto (alto, medio, bajo).

Existió dificultad el momento de estimar el impacto en el caso de reputación y multas para algunas de las amenazas, por lo que se decidió consultar el criterio del Gerente General de la empresa para poder realizar estas estimaciones.

De manera particular se identifica la pérdida o interrupción del activo crítico en cada área de interés como lo más importante a tomar en cuenta en caso de una amenaza.

3.4.1.2 Establecer criterios de evaluación basado en la frecuencia

Tabla 49: Hoja de Trabajo: Criterios basados en la frecuencia

	1. Piense en lo que constituye un riesgo alto, medio y bajo de la ocurrencia de amenazas a los activos críticos de la organización.				
	Alto				**Medio**
Tiempo entre eventos	*Diario*	*Semanal*	*Mensual*	*Cuatro veces al año*	*< 4 veces al año*
Frecuencia analizada	*365*	*52*	*12*	*4*	*<4*

	2. Dibuje líneas que separen alto de medio y medio de bajo				
Medio	**Bajo**				
Una vez al año	*< 1 vez al año*	*Una vez cada 5 años*	*Una vez cada 10 años*	*Una vez cada 20 años*	*Una vez cada 50 años*
1	*<1*	*0.2*	*0.1*	*0.05*	*0.02*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 150-151

Se definió la frecuencia utilizando la Hoja de Trabajo: Criterios basados en la frecuencia basándose en su experiencia y conocimientos, así como la limitada información histórica que tenían de amenazas para definir el criterio a utilizar para estimar si la ocurrencia de amenazas al Portal de Gerencia es alto, medio o bajo.

Se definió un límite alto si la ocurrencia de una amenaza sucedía más de cuatro veces al año, medio si la ocurrencia es entre una y cuatro veces al año y baja si ocurría menos de una vez al año.

3.4.1.3 Evaluar probabilidades de amenaza

Tabla 50: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red. Probabilidad

Actores con acceso a la red – Probabilidad									
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*						**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**		**Valor**	**Confianza**		
							Muy	**Algo**	**Nada**
Portal	Red	Adentro	Accidental	Revelación		*B*		*X*	
				Modificación		*B*		*X*	
			Premeditado	Pérdida		*M*		*X*	
				Interrupción		*M*		*X*	
		Afuera	Accidental	Revelación		*M*		*X*	
				Modificación		*M*		*X*	
				Pérdida		*M*		*X*	
				Interrupción		*M*		*X*	
			Premeditado	Revelación		*M*		*X*	
				Modificación		*M*		*X*	
				Pérdida		*M*		*X*	
				Interrupción		*B*		*X*	
			Accidental	Revelación		*M*		*X*	
				Modificación		*M*		*X*	
				Pérdida		*M*		*X*	
				Interrupción		*M*		*X*	
			Premeditado	Revelación		*M*		*X*	
				Modificación		*M*		*X*	

	Pérdida	*M*		*X*	
	Interrupción	*M*		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 94, 119

Tabla 51: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema. Probabilidad

Problemas del Sistema – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
Portal	Defectos de software	Revelación	*B*	*X*		
		Modificación	*M*	*X*		
		Pérdida	*B*	*X*		
		Interrupción	*B*	*X*		
	El sistema se cae	Revelación	*B*	*X*		
		Modificación	*A*	*X*		
		Pérdida	*M*	*X*		
		Interrupción	*A*	*X*		
	Defectos de hardware	Revelación	*B*	*X*		
		Modificación	*A*	*X*		
		Pérdida	*M*	*X*		
		Interrupción	*A*	*X*		
	Código malicioso	Revelación	*B*	*X*		
		Modificación	*B*	*X*		
		Pérdida	*B*	*X*		

	Interrupción	*B*	*X*		

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 121

Tabla 52: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Probabilidad

Otros Problemas – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
Portal	Problemas con el suministro de energía	Revelación	*B*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*M*		*X*	
		Interrupción	*A*		*X*	
	Problemas de telecomunicaciones	Revelación	*B*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*A*		*X*	
		Interrupción	*A*		*X*	
	Problemas con sistemas de terceros	Revelación	*M*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*M*		*X*	
		Interrupción	*M*		*X*	
	Desastres naturales	Revelación	*B*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*M*		*X*	

	Interrupción	*A*		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 128

Tabla 53: Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Probabilidad

Otros Problemas – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
Portal	Personas clave permiso temp.	Revelación	*B*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*A*		*X*	
		Interrupción	*A*		*X*	
	Personas clave que renuncian	Revelación	*B*		*X*	
		Modificación	*M*		*X*	
		Pérdida	*A*		*X*	
		Interrupción	*A*		*X*	

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 132

Usando la Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Probabilidad con la ayuda del equipo de trabajo y el Gerente General de la organización se evaluó la probabilidad de que ocurra una amenaza y se determinó el nivel de confianza de este estimado, los resultados son los siguientes:

Para cualquier amenaza que ocurra por problemas del sistema como defectos de software, si el sistema se cae, defectos de hardware o código malicioso el equipo de análisis se mostró muy confiado al realizar estimados de probabilidades de ocurrencia de estas amenazas en el futuro, tomando especial atención si se trata de un defecto de hardware o si el sistema se cae ya que consideran hay mayor probabilidad de que ocurra alguna modificación o interrupción en el activo.

Para realizar estimados de probabilidades de amenaza causadas por actores con acceso a la red, el equipo se muestra poco confiado, ya que es difícil predecir el comportamiento de la gente sin embargo, consideran que la principal amenaza se presentaría con alguna persona externa a la organización que lo haga accidentalmente o con intención de causar daño.

En el caso de amenazas presentadas por problemas con el suministro de energía, telecomunicaciones, problemas con sistemas de terceros o desastres naturales se considera que la probabilidad de que suceda en el futuro es media para cada caso. El equipo se mostró poco confiado al realizar estas estimaciones.

Finalmente, la probabilidad de que ocurra una amenaza si una persona clave en la organización tome un permiso temporal o una persona clave en la organización renuncie es alta si el resultado es pérdida o interrupción; en este caso igualmente el equipo de análisis se mostró poco confiado en estas estimaciones.

3.5.1 Proceso S5: Desarrollo de estrategias y planes de mitigación

3.5.1.1 Describir estrategia de protección actual

Tabla 54: Hoja de Trabajo: Conocimiento de seguridad y entrenamiento

¿Qué tan formal es la estrategia de capacitación de su organización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Estrategia de Protección		
La organización cuenta con una estrategia de capacitación documentada que incluye una evaluación del conocimiento de seguridad para la sensibilización y la formación en materia de seguridad para las tecnologías de apoyo.	Actual	(Cambiar)
La organización tiene una estrategia de capacitación informal e indocumentada.	(Actual)	Cambiar

¿Qué tan seguido se realizan entrenamientos de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Evaluar el conocimiento de Seguridad		
Se proveen entrenamientos periódicos sobre seguridad que a todos los empleados 1 vez cada año.	Actual	(Cambiar)
Se provee entrenamiento sobre seguridad a personas nuevas en la organización como parte de sus actividades de orientación.	Actual	Cambiar
La organización no provee un entrenamiento sobre seguridad. Cada miembro del personal aprende sobre problemas de seguridad por sí mismo.	(Actual)	Cambiar

¿En qué medida se requiere que los miembros del área de TI asistan a un entrenamiento relacionado con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento relacionado con Seguridad		
Los miembros del área de TI deben asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	Actual	Cambiar
Los miembros del área de TI pueden asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen si ellos lo piden.	Actual	(Cambiar)
La organización no provee oportunidades para que miembros del área de TI asistan a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	(Actual)	Cambiar

¿Qué tan formal es el mecanismo de su organización para proveer actualizaciones periódicas de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Actualizaciones periódicas de Seguridad		
La organización tiene mecanismos formales para proveer miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	Actual	(Cambiar)
La organización no tiene un mecanismo para proveer a miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	(Actual)	Cambiar

¿Cuál es el mecanismo oficial de su organización para verificar que el personal reciba capacitación? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Verificación del Entrenamiento		
La organización tiene mecanismos formales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual	Cambiar
La organización tiene mecanismos informales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual	(Cambiar)
La organización no tiene mecanismos para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	(Actual)	Cambiar

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 156-158

Tabla 55: Hoja de Trabajo: Estrategia de protección para el manejo colaborativo de la seguridad

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con colaboradores y socios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Colaboradores y Socios		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con colaboradores y socios.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con colaboradores y socios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con colaboradores y socios.	Actual	(Cambiar)
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con colaboradores y socios.	(Actual)	Cambiar

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con contratistas y subcontratistas? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Contratistas y Subcontratistas		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con contratistas y subcontratistas. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con contratistas y subcontratistas.	Actual	(Cambiar)
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	(Actual)	Cambiar

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con proveedores de servicios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Proveedores de Servicios		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con proveedores de servicios.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con proveedores de servicios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con proveedores de servicios.	Actual	(Cambiar)
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con proveedores de servicios.	(Actual)	Cambiar

¿Hasta qué punto la organización comunica formalmente sus requisitos de protección de la información a terceras partes? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Requerimientos		
La organización documenta los requisitos de protección de la información y las comunica explícitamente a terceras partes.	Actual	Cambiar
La organización comunica informalmente los requisitos de protección de información a terceras partes.	Actual	(Cambiar)
La organización no comunica sus requisitos de protección de información a terceras partes.	(Actual)	Cambiar

¿Hasta qué punto la organización verifica que terceras partes estén cumpliendo con los requisitos de protección de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Verificación		
La organización tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual	Cambiar
La organización tiene mecanismos informales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual	(Cambiar)
La organización no tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	(Actual)	Cambiar

¿Hasta qué punto el programa de entrenamiento sobre conocimiento de seguridad de su organización incluye manejo colaborativo de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Conocimiento del Personal		
El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año.	Actual	Cambiar
El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a los nuevos empleados como parte de sus actividades de orientación.	Actual	Cambiar
El programa de entrenamiento sobre conocimiento de seguridad de la organización no incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año. Los miembros del personal aprenden sobre manejo colaborativo de la seguridad por si mismos.	Actual	Cambiar

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 159-162

Tabla 56: Hoja de Trabajo: Estrategia de protección para monitorear y auditar seguridad física

¿Quién es actualmente responsable para monitorear y auditar la seguridad física? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Responsabilidad						
Tarea:	Actual			Cambiar		
	Interno	Externo	Combinado	Interno	Externo	Combinado
Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware.				*X*		
Monitorear acceso físico controlado por hardware.				*X*		
Monitorear acceso físico controlado por software.				*X*		
Monitorear acceso físico a áreas de trabajo restringidas.	*X*					
Revisar los registros de monitoreo periódicamente.				*X*		
Investigar y monitorear cualquier actividad inusual no identificada.				*X*		

¿Hasta qué punto son los procedimientos de esta área formalmente documentados? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Procedimientos		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización ha documentado formalmente planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual	(Cambiar)
La organización ha documentado formalmente algunos planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software. Algunas políticas y procedimientos son informales y no son documentados.	Actual	Cambiar
La organización tiene planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software que son informales y no documentados.	(Actual)	Cambiar

¿Hasta qué punto se requiere que el personal de su organización asista a entrenamientos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
Miembros designados del personal están obligados a asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual	Cambiar
Miembros designados del personal pueden asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software si ellos lo piden.	Actual	(Cambiar)
La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	(Actual)	Cambiar

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 163-170

Tabla 57: Hoja de Trabajo: Estrategia de protección para autenticación y autorización

¿Quién es actualmente responsable de la autenticación y autorización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Responsabilidad						
Tarea:	Actual			Cambiar		
	Interno	Externo	Combinado	Interno	Externo	Combinado
Implementar control de acceso (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	*X*					
Implementar autenticación de usuarios (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	*X*					
Establecer y terminar acceso a sistemas e información para ambos individuos y grupos.				*X*		

¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Procedimientos		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización ha documentado formalmente autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar
La organización ha documentado formalmente autorización y autenticación de algunos procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red. Algunos procedimientos en esta área son informales y no están documentados.	Actual	Cambiar
La organización tiene procedimientos informales y no documentados para la autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar

¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
Miembros designados del personal están obligados a asistir a entrenamientos para implementar medidas tecnológicas para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar
Miembros designados del personal pueden asistir a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red si ellos lo piden.	Actual	(Cambiar)
La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	(Actual)	Cambiar

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 171-176

Tabla 58: Hoja de Trabajo: Estrategia de protección para políticas de seguridad y regulaciones

¿Hasta qué punto están formalmente documentadas las estrategias de protección relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Políticas Documentadas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene un conjunto integral de políticas relacionadas con seguridad formalmente documentadas.	Actual	Cambiar
La organización tiene un conjunto integral de políticas relacionadas con seguridad informalmente documentadas.	Actual	(Cambiar)
Las políticas relacionadas con seguridad de la organización son informales y no están documentadas.	(Actual)	Cambiar

¿Qué tan formal es el mecanismo de su organización para crear y actualizar sus políticas relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Manejo de Políticas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene un mecanismo formal para crear y actualizar su política relacionada con seguridad.	Actual	Cambiar
La organización tiene un mecanismo formal para crear su política relacionada con seguridad. La organización tiene un mecanismo informal y no documentado para actualizar su política relacionada con seguridad.	Actual	(Cambiar)
La organización tiene un mecanismo informal y no documentado para crear y actualizar su política relacionada con seguridad.	(Actual)	Cambiar

¿Qué tan formal son los procedimientos de su organización para aplicar sus políticas relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Aplicación de Políticas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene procedimientos formales para aplicar su política relacionada con seguridad. Estos procedimientos aplicados son aplicados y seguidos constantemente.	Actual	Cambiar
La organización tiene procedimientos formales para aplicar su política relacionada con seguridad. Estos procedimientos aplicados nunca se siguen.	Actual	(Cambiar)
La organización tiene un mecanismo informal y no documentado para aplicar su política relacionada con seguridad.	(Actual)	Cambiar

¿Qué tan formales son los procedimientos de su organización para cumplir con las políticas y regulaciones relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Políticas y Cumplimiento del Reglamento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene procedimientos formales para cumplir con políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro.	Actual	Cambiar
La organización tiene procedimientos formales para cumplir con ciertas políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro. Algunos procedimientos en esta área son informales y no están documentados.	Actual	(Cambiar)
La organización tiene procedimientos informales y no documentados para cumplir con políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro.	(Actual)	Cambiar

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 177-180

La Hoja de Trabajo: Estrategia de Protección se ha utilizado para que se discuta las actuales estrategias de protección y vulnerabilidades de cada área en la organización. La estrategia de protección describe los distintos procesos que se utilizan para realizar diferentes prácticas de seguridad enfocándose en conocer hasta qué grado cada proceso está formalmente definido; en esta hoja de trabajo el equipo de análisis define también qué cambios se debería hacer a cada área en la organización para mejorar su estrategia y capacitación en seguridad.

Se debe tener en cuenta que en una organización se puede presentar uno de estos escenarios: "la compañía se desempeña muy bien en un área, pero tienen procesos muy informales, o una organización tiene un amplio margen de mejora a pesar de tener políticas y procedimientos muy formales"[48]

La estrategia de protección actual se describe a continuación:

- **Conocimiento de seguridad y entrenamiento:** El equipo de análisis cree que su actual estrategia de protección no está definida apropiadamente para manejar los problemas del día a día que puedan surgir, adicionalmente el personal no ha recibido un entrenamiento formal sobre seguridad y tampoco existen mecanismos para rastrear y monitorear que los miembros del personal se entrenen en temas de seguridad. Mejorar esta área debe reducir las fuentes accidentales de amenazas internas.

- **Manejo colaborativo de la seguridad:** Actualmente no existe una política para proteger información cuando se trabaja con colaboradores y socios, contratistas y subcontratistas y proveedores de servicios; tampoco se cuenta con mecanismos formales para verificar que organizaciones de terceros cumplan con los requerimientos de la empresa.

  No hay entrenamiento a disposición del personal para el manejo colaborativo de seguridad, políticas y procedimientos.

- **Monitorear y auditar seguridad física:** Hubo cierta preocupación por los miembros del equipo al analizar los problemas de seguridad física existían en Pirámide Digital ya que no existen planes para controlar áreas de trabajo, hardware y software y tampoco se provee

[48] Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 11

entrenamiento en esta área. Con respecto a la seguridad física, el departamento de seguridad del edificio World Trade Center es responsable del acceso físico a la empresa en la oficina en Quito y esta actividad está totalmente controlada.

- **Autenticación y autorización:** En la organización no estaba usando un medio consistente para controlar el acceso a redes y no se han definido procedimientos para restringir acceso a usuarios ni que permisos debe tener que persona, el equipo estaba preocupado por las posibles consecuencias de estas cuestiones.

- **Políticas de seguridad y regulaciones:** No existen políticas documentadas relacionadas con seguridad, un mecanismo formal para crear y manejar políticas ni procedimientos formales para cumplir con políticas de seguridad, leyes, regulaciones o requisitos.

3.5.1.2 Desarrollar plan de mitigación

Tabla 59: Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Conocimiento de seguridad y entrenamiento*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*
Proveer entrenamiento sobre seguridad a personas nuevas en la organización como parte de sus actividades de orientación y a todo el personal una vez al año.	*La política actual de Pirámide Digital no provee un entrenamiento sobre seguridad, cada miembro del personal aprende sobre problemas de seguridad por sí mismo. Debe existir un entrenamiento de seguridad periódico.*
Permitir que miembros del personal asistan a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen si ellos lo piden.	*No hay entrenamiento relacionado con tecnologías utilizadas en la organización.*
El encargado de cada departamento deberá tener una lista para rastrear qué persona asistió a un entrenamiento y cuando asistió.	*Se debe implementar un mecanismo para rastrear y verificar que los miembros del personal reciban entrenamiento.*
Establecer políticas y procedimientos para la determinación de roles y responsabilidades del personal.	*Con esta actividad se evitará que posibles errores humanos pongan en riesgo al activo.*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*
Gerente General *Gerente de Tecnología*	*Para que exista un entrenamiento periódico se necesita que haya compromiso por parte de la Gerencia General y que se destinen fondos para esta actividad.*
Gerente General *Gerente de Tecnología*	*Debe haber fondos para que esta actividad se realice.*
Gerencia General y los encargados de cada departamento	*Todos los encargados de cada departamento de la empresa deben participar en esta actividad para tener un control adecuado.*
Gerente de Tecnología	*Todo el personal debe colaborar.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 182-183

Tabla 60: Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Manejo colaborativo de la seguridad*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*
Proveer entrenamiento sobre manejo colaborativo de seguridad a personas nuevas en la organización como parte de sus actividades de orientación y a todo el personal una vez al año.	*La política actual de Pirámide Digital no provee un entrenamiento sobre seguridad, cada miembro del personal aprende sobre problemas de seguridad por sí mismo. Debe existir un entrenamiento de seguridad periódico.*
Designar a un miembro del área IT como punto de contacto para comunicar ciertos requerimientos cuando se trabaja con colaboradores y socios, contratistas y subcontratistas, proveedores de servicios.	*Actualmente no se hace nada con respecto de comunicar requerimientos para trabajar con terceros.*
Designar a un miembro del área IT como punto de contacto para verificar que organizaciones de terceros, servicios de seguridad externos y tecnologías cumplan con sus requerimientos.	*Actualmente no se hace nada con respecto de verificar que organizaciones de terceros cumplan con sus requerimientos.*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*
Gerente de Tecnología	*La Gerencia General debe patrocinar esta actividad y la Gerencia de Tecnología debe asignar a una persona de si equipo como punto de contacto.*
Gerente de Tecnología	*La Gerencia General debe patrocinar esta actividad y la Gerencia de Tecnología debe asignar a una persona de si equipo como punto de contacto.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 182-183

Tabla 61: Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Monitorear y auditar seguridad física*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*
Documentar formalmente procedimientos para monitorear acceso físico a hardware y software para que se asegure que se apliquen por todos los miembros del personal. Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware y software. *Monitorear el acceso físico mediante el uso de credenciales que permitan controlar, limitar, monitorear y auditar el acceso a distintas áreas de la oficina.*	*No existen planes para monitorear el acceso físico, hardware y software sin embargo, algunos procesos se monitorean informalmente.*
Asignar a una persona encargada de monitorear cualquier actividad inusual.	*No hay nadie responsable de monitorear actividades inusuales.*
Definir políticas en caso de falla de un equipo.	*No hay políticas definidas o documentadas.*
Planificar mantenimiento periódico del servidor donde se aloja el Portal de Gerencia.	*Se realiza mantenimiento sin embargo no se documenta ningún cambio.*
Inventario de estaciones de trabajo y equipos y seguro.	*No existe un inventario actualizado, no se ha contratado ningún seguro en caso de protección.*
Documentar estrategia para control de acceso y capacitación del personal.	*No hay ninguna estrategia definida.*
Mecanismo de vigilancia.	*En ejecución, pero no al 100%*
Establecer políticas para el Primary Domain Control (servidor) para instalación de software no autorizado.	*No se ha considerado realizar este cambio.*
Paquetes de actualización a través de la consola del servidor (Wake On LAN).	*No se ha considerado realizar este cambio.*
Asignar a una persona que asista a	*No se provee entrenamientos para monitorear y*

entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software una vez al año.	*auditar la seguridad física.*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*
Miembros del área de TI	*Entrenar al personal involucrado en cómo realizar planes y monitorear apropiadamente el acceso físico.*
Gerencia TI	*Entrenar al encargado.*
Gerencia TI	*Definir un responsable.*
Gerencia TI	*Entrenar al responsable para establecer políticas de actualización.*
Gerencia TI	*Definir un responsable.*
Gerencia TI	*Entrenamiento y capacitación.*
Gerencia TI	*Asignar a un responsable para que se termine la implementación de cámaras de vigilancia.*
Gerencia TI *Gerencia General*	*Asignar fondos para la implementación.*
Gerencia TI *Gerencia General*	*Asignar fondos para la implementación.*
Gerencia General *Miembros del área de TI*	*Asignar fondos para entrenamiento sobre acceso físico.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 182-183

Tabla 62: Hoja de Trabajo: Autenticación y autorización

Área de Mitigación: *Autenticación y autorización*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*
Asignar responsables encargados de implementar control de acceso y autenticación de usuarios y documentar la autorización y autenticación de procedimientos.	*Miembros del área de TI deben estar involucrados y participar en implementar control de acceso al Portal de Gerencia ya que actualmente no se conoce quién debe tener acceso qué.*
Asignar a una persona que asista a entrenamientos para restringir a usuarios de acceso a información, sistemas susceptibles y servicios específicos.	*No se provee entrenamientos para esta actividad.*
Revisar las estaciones de trabajo para asegurarse que el acceso a las mismas hibernen automáticamente después de un cierto tiempo y pidan ingresar la contraseña.	*En muchas ocasiones hay clientes visitando la organización y como en varios casos se comparte el espacio físico personas no autorizadas pueden acceder a información en estas maquinas.*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*
Miembros del área de TI	*Entrenar al personal de TI para implementar y documentar control de acceso y autenticación de usuarios*
Gerencia General *Miembros del área de TI*	*Asignar fondos para entrenamiento sobre acceso físico.*
Gerencia General *Gerencia de Tecnología*	*La Gerencia General debe patrocinar esta actividad y en colaboración con el Gerente de Tecnología deben asignar a un miembro del área de TI para que realice este cambio.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 182-183

Tabla 63: Hoja de Trabajo: Políticas de seguridad y regulaciones

Área de Mitigación: *Políticas de seguridad y regulaciones*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*
Incluir información sobre políticas y procedimientos en el entrenamiento de seguridad.	*Nadie tiene clara la actual política de seguridad, todas las dudas del personal se deben despejar en un entrenamiento de seguridad dictado a todo el personal.*
Crear procedimientos para hacer cumplir políticas de seguridad (Envío de correos al personal recordándoles políticas básicas de seguridad)	*La conducta de las personas con respecto a la seguridad solo cambiará si entienden cómo manejar y hacer cumplir los procedimientos de las políticas de seguridad de la empresa.*
Definir planes de recuperación y contingencia.	*Es importante que la empresa continúe funciones criticas en caso de interrupción parcial .*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*
Gerencia General	*La Gerencia General debe patrocinar esta actividad.*
Gerencia General	*La Gerencia General debe patrocinar esta actividad.*
Gerencia General *Gerencia Tecnología*	*La Gerencia General debe patrocinar esta actividad y asignar a un miembro de TI.*

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 182-183

3.5.1.3 Identificar cambios a la estrategia de protección

Después de revisar las hojas de trabajo de Protección de Seguridad para determinar los cambios desencadenados por las actividades de mitigación; estas actividades se las describe a continuación:

- Contar con un programa de entrenamiento sobre conocimiento de seguridad que incluya manejo colaborativo de seguridad, políticas y procedimientos que se realizan una vez al año y al que asista todo el personal.
- Establecer políticas y procedimientos para la determinación de roles y responsabilidades del personal, los cuales se deben cumplir y respetar.
- Designar a un miembro del área de TI como punto de contacto para comunicar requerimientos de la organización al trabajar con colaboradores, socios, organizaciones de terceros y servicios externos.
- Documentar formalmente planes y procedimientos para monitorear el acceso físico al edificio y la oficina de la empresa
- Monitorear el acceso físico mediante el uso de credenciales que permiten controlar, limitar, monitorear y auditar el acceso a distintas áreas en las oficinas.
- Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware.
- Mantener registros de mantenimiento para documentar reparaciones y modificaciones al software.
- Asignar a una persona encargada de monitorear cualquier actividad inusual quien además deberá investigar a fondo esta actividad y redactar un reporte en caso de que ocurra un incidente sospechoso.
- Definir políticas en caso de falla de algún equipo clave para que siempre se cuente con un equipo respaldo para que el usuario afectado retome sus actividades en el menor tiempo posible.
- Planificar mantenimiento periódico del servidor donde se encuentra alojado el Portal de Gerencia, esto debe estar documentado formalmente y se debe definir un encargado de realizar esta actividad.

- Definir y actualizar periódicamente un inventario de las estaciones de trabajo y equipos con los que cuenta la empresa, para tener control del estado de los mismos.
- Implementar un mecanismo de vigilancia mediante el uso de cámaras para controlar el acceso de personas no autorizadas a las oficinas.
- Establecer políticas para el servidor principal de la organización para que ninguna persona pueda instalar software de tal manera, el único autorizado a hacer instalaciones en los equipos de trabajo es el administrador de la red.
- Incorporar paquetes de actualizaciones a través de la consola del servidor principal para que en la noche los equipos de trabajo se enciendan automáticamente mediante el uso de Wake On LAN y se distribuyan paquetes de actualización de software, antivirus, malware, etc. y se asegure que todos los equipos tengan las mismas y últimas versiones del software actualizado.
- Contratar un seguro para las estaciones de trabajo y equipos de la empresa.
- Documentar formalmente la estrategia que se va a utilizar para controlar el acceso y la autenticación de usuarios ya sea mediante una contraseña que debe ser cambiada periódicamente, tarjetas de identidad inteligentes o un sistema basado en una característica física del usuario.
- Capacitar al personal para que tomen medidas básicas de seguridad para minimizar el acceso no autorizado a sus equipos.
- Asignar responsables encargados de implementar y documentar control de acceso y autenticación de usuarios.
- Cambiar la configuración de autenticación de usuarios y definir qué persona que pertenece a la organización debe tener acceso a cierta información.
- Revisar las estaciones de trabajo para asegurarse que el acceso a las mismas hibernen automáticamente después de un cierto tiempo y pidan ingresar la contraseña.
- Incluir información sobre políticas y procedimientos en el entrenamiento de seguridad.
- Establecer políticas y procedimientos para la planificación de respaldos periódicos de toda la información sensible que se maneja por los usuarios.

- Asegurarse que le personal conozca los nuevos procedimientos de seguridad, esto se puede realizar mediante el envío de correos al personal recordándoles políticas básicas de seguridad.
- Definir planes de recuperación de desastres y continuidad del negocio que permitan garantizar que la organización continuará con sus funciones críticas en caso de haber sido interrumpidas parcial o totalmente.
- Asignar a miembros del personal quienes asistirán a un entrenamiento sobre restricción de usuarios al acceso de información, sistemas susceptibles, servicios específicos, monitoreo del acceso físico, áreas de trabajo, hardware y software.

3.5.1.4 Identificar siguientes pasos

Tabla 64: Hoja de Trabajo: Identificar siguientes pasos

Considere:

- *Contribuir fondos para las actividades de seguridad de la información.*
- *Asignar personal para las actividades de seguridad de la información.*
- *Asegurarse que los funcionarios dispongan de tiempo suficiente asignado a las actividades de seguridad de la información.*
- *Permitir al personal recibir entrenamiento sobre seguridad de la información.*
- *Hacer que la seguridad de la información sea una prioridad estratégica.*

Gestión para la mejora de la Seguridad	**Monitorear la implementación**	**Ampliar la actual evaluación de riesgos en la seguridad de la información**	**Siguiente evaluación de riesgos en la seguridad de la información**
¿Qué debe hacer la Gerencia para apoyar la implementación de los resultados de Octave-S?	*¿Qué debe hacer la información para rastrear el progreso y asegurar que los resultados de esta evaluación se implementen?*	*¿Expendería la actual evaluación OCTAVE-S para incluir activos críticos adicionales? ¿Cuáles?*	*¿Cuándo conducirá la organización su siguiente evaluación OCTAVE-S?*
La Gerencia General de Pirámide Digital debe: • *Asignar fondos para implementar el plan de mitigación.* • *Hacer que la seguridad de la información se convierta en una prioridad de la empresa.* • *Los Gerentes de las distintas áreas de*	*Cada persona a la que se le asigne cumplir una actividad de mitigación se debe hacer responsable de fijar un cronograma e implementar cada plan, adicionalmente se debe redactar un reporte a presentarse al concluir con dicha actividad.*	*No se ha identificado actividades para expandir la actual evaluación de riesgos.*	*La siguiente evaluación se realizará en tres años.*

la organización se deben asegurar que el personal cuente con tiempo suficiente para participar en cualquier actividad relacionada con seguridad que se les asigne. • *Asignar responsables encargados de de implementar y documentar control de acceso y autenticación de usuarios.* • *Asignar responsables encargados de monitorear el acceso físico al edificio, áreas de trabajo, hardware.* • *Cambiar al procedimiento para cumplir políticas de seguridad.*			

Realizado por: Olga Páez en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Version 1.0, Volume 10: Example Scenario. Pittsburgh, PA, Carnegie Mellon Software Engineering Institute, 2005, 196-197

CAPITULO CUATRO

EVALUACIÓN DEL PLAN DE ACCIÓN Y ESTRATEGIA DE PROTECCIÓN

En este capítulo se presentan el informe preliminar e informe final y ejecutivo dirigido al Gerente General de Pirámide Digital Cía. Ltda. quien es la persona encargada de monitorear la implementación de los resultados obtenidos durante la ejecución de la evaluación de seguridad a la empresa.

4.1 Elaboración de Informe Preliminar y validación del mismo por la empresa

Quito, septiembre del 2013

Señor Ingeniero

Pablo Páez, PhD

Gerente General

Pirámide Digital. Cía. Ltda.

De mis consideraciones:

Por medio de la presente, pongo a su disposición el análisis utilizando las metodologías COBIT 4.1 para analizar la situación actual de la empresa y la evaluación de amenazas críticas, activos y vulnerabilidades que propone OCTAVE-S (Operationally Critical Threat, Asset and Vulnerability Evaluation) la que se ha realizado con ayuda de personas que trabajan en la empresa, en la que se ha asumido la responsabilidad de establecer la estrategia de seguridad de la organización analizando la información de la empresa para producir una estrategia de protección y planes de mitigación basados exclusivamente en los riesgos de seguridad operacional de la organización.

El equipo de trabajo y análisis está conformado por:

- Olga Páez
- Mario Morillo
- Olga Obando
- Guillermo Obando

El informe redactado en base a COBIT 4.1 y OCATVE-S; COBIT4.1 describe la situación actual de la organización utilizando matrices de madurez para evaluar los siguientes dominios: planeación y organización, adquisición e implementación, entrega y soporte y monitoreo y evaluación. OCTAVE –S describe los resultados de la evaluación y se basa en cuatro ejes principales: conocimiento de seguridad y entrenamiento, manejo colaborativo de la seguridad, monitoreo y auditoría de la seguridad física y autenticación y autorización

A más de presentarle el informe final e informe ejecutivo, me comprometo a aclarar cualquier duda o a ampliar cualquier información que no se encuentre totalmente sustentada.

Le reitero, que la información que se presenta a continuación estará únicamente disponible para la empresa y no será divulgada a ninguna persona bajo ninguna circunstancia.

Muchas gracias por su atención y tiempo.

4.2 Elaboración del Informe Final

El presente informe muestra los resultados de la evaluación que establece COBIT 4.1 para realizar un análisis de la situación de la empresa y OCTAVE-S para realizar una evaluación de riesgos y seguridad. A continuación se presentan los resultados obtenidos:

Situación actual de la empresa:

En base a las Matrices de Madurez aplicadas a los procesos seleccionados de Cobit 4.1 se ha encontrado lo siguiente:

Dominio Planeación y Organización

Nivel de Madurez: Uno

Es necesario implementar un plan estratégico, en el que se defina un proceso que permita identificar y realizar actualizaciones del mismo. Se debe implementar una política de cómo y cuándo se va a realizar la planeación estratégica de TI, la que debe ser conocida por todo el equipo de trabajo y se debe garantizar que sea el plan que se realice sea factible y estructurado. La planeación estratégica debe ser discutida en reuniones con la Dirección y se debe contar con técnicas y estándares comunes para el desarrollo de la infraestructura tecnológica. La estrategia general de TI, debe incluir una definición de los riesgos a los que está expuesta la organización.

Es importante que se difunda la necesidad de la planeación tecnológica para que exista un enfoque en generar soluciones a problemas técnicos que permitan satisfacer las necesidades del negocio Los riesgos de TI relacionados al día a día a las diferentes operaciones de TI, deben ser discutidos siempre en las reuniones con la Gerencia General; además debe existir un enfoque de evolución de riesgos en desarrollo y debe ser implementado en discreción del gerente de TI. El personal encargado de realizar la planeación, debe potenciar sus habilidades sobre planeación tecnológica, a través de un aprendizaje y una aplicación repetida de las técnicas, así como un entrenamiento formal. Debe también existir comunicación de los roles de todos los empleados y sus responsabilidades, especialmente de los empleados de la unidad de TI, quienes deben tener roles formalizados, los cuales deben ser cumplidos a cabalidad..

La unidad de TI debe organizarse de tal manera, que sea capaz de responder de forma táctica y oportuna a las necesidades de los clientes y los distintos proveedores, la organización de la unidad de TI debe ser estructurada de tal manera, que las decisiones dependan del conocimiento y las habilidades de los individuos clave; debe contar con técnicas emergentes comunes para administrar la organización de TI y sus relaciones con los demás departamentos, además debe haber un deseo emergente del personal de entender que los riesgos de TI son importantes y necesarios y deben ser siempre considerados.

Dominio Adquisición e Implementación

Nivel de Madurez: Uno

Se debe crear una conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Estas políticas y procedimientos deben ser integrados parcialmente con el proceso general de adquisición de la organización del negocio, los que deben ser utilizados en proyectos menores y deben ser usados como base para luego implementarlos en cada proyecto que maneje la empresa. Se debe lograr que el proceso de administración de cambio no sea un proceso informal para evitar que el proceso no sea estructurado, rudimentario y propenso a errores, la empresa debe reconocer la importancia de administrar sus proveedores y las distintas relaciones entre ellos.

Se deben determinar responsabilidades para administrar correctamente la adquisición y contratos de TI según la experiencia de cada persona a cargo y que la exactitud de la documentación de la configuración sea consistente y no sea de planeación limitada, de tal manera que la evolución del impacto de los cambios de TI sean previos al cambio.

Dominio Entrega y Soporte

Nivel de Madurez: Uno

La empresa debe desarrollar las políticas de seguridad, pues es necesario que exista la necesidad de administrar los niveles de servicio aun si el proceso sea informal y reactivo. Para la definición y administración de los servicios, se debe definir la responsabilidad y la

rendición de cuentas, las que se deben asignar a un coordinador de seguridad de TI, aunque en este nivel de madurez, la autoridad del coordinador es limitada. Se deben definir medidas para medir el desempeño, para poder analizar la información que producen los sistemas relevantes al aspecto de seguridad. La seguridad del departamento de TI se debe ver primordialmente como una responsabilidad y disciplina del área de TI.

Se deben generar reportes de incidentes que estén integrados con la administración de datos de configuración, para que se pueda resolver los problemas reportados, además de emplear mecanismos automáticos de advertencia y detección, para su evaluación continua, se debe contar con suficientes pistas de auditoría de problemas y soluciones, los cuales deben ser integrados con la administración de datos de configuración, permitiendo de esta manera, la oportuna resolución de los problemas reportados, también hay que contar con información de los problemas pasados que ha enfrentado la empresa y posibles problemas futuros, para optimizar la solución de problemas internos de la organización.

Dominio Monitoreo y Evaluación

Nivel de Madurez: Cero

La empresa debe contar con reportes útiles, oportunos y precisos, los que se deben estandarizar y normalizar; además se debe definir estándares de recolección y evaluación de acuerdo a las necesidades de los proyectos y procesos específicos de TI, para tener un mejoramiento continuo de los distintos servicios que brinda la empresa, se debe realizar evaluaciones de satisfacción al usuario, a más de establecer programas de mejora continua dentro de la empresa.

La compañía debe implementar procedimientos para monitorear la efectividad de los controles internos, establecer responsabilidades para el control interno, realizar un monitoreo permanente de control interno y asignar de manera formal las tareas para monitorear la efectividad de los controles internos y evaluarlos en base a la necesidad de los servicios de información.

Los resultados encontrados al aplicar OCATVE-S son los siguientes:

Estrategia de protección actual:

- **Conocimiento de seguridad y entrenamiento:** La actual estrategia de protección no está definida apropiadamente para manejar los problemas del día a día que puedan surgir, adicionalmente el personal no ha recibido un entrenamiento formal sobre seguridad y tampoco existen mecanismos para rastrear y monitorear que los miembros del personal se entrenen en temas de seguridad. Mejorar esta área debe reducir las fuentes accidentales de amenazas internas.

- **Manejo colaborativo de la seguridad:** Actualmente no existe una política para proteger información cuando se trabaja con colaboradores y socios, contratistas y subcontratistas y proveedores de servicios; tampoco se cuenta con mecanismos formales para verificar que organizaciones de terceros cumplan con los requerimientos de la empresa.
  No hay entrenamiento a disposición del personal para el manejo colaborativo de seguridad, políticas y procedimientos.

- **Monitorear y auditar seguridad física:** No existen planes para controlar áreas de trabajo, hardware y software y tampoco se provee entrenamiento en esta área. Con respecto a la seguridad física, el departamento de seguridad del edificio World Trade Center es responsable del acceso físico a la empresa en la oficina en Quito y esta actividad está totalmente controlada.

- **Autenticación y autorización:** En la organización no se estaba usando un medio consistente para controlar el acceso a redes y no se han definido procedimientos para restringir acceso a usuarios ni que permisos debe tener que persona, el equipo estaba preocupado por las posibles consecuencias de estas cuestiones.

- **Políticas de seguridad y regulaciones:** No existen políticas documentadas relacionadas con seguridad, un mecanismo formal para crear y manejar políticas ni procedimientos formales para cumplir con políticas de seguridad, leyes, regulaciones o requisitos.

Después de realizar la evaluación de seguridad actual de la organización se realizo un plan de mitigación con actividades que se describen a continuación:

- Contar con un programa de entrenamiento sobre conocimiento de seguridad que incluya manejo colaborativo de seguridad, políticas y procedimientos que se realizan una vez al año y al que asista todo el personal.
- Establecer políticas y procedimientos para la determinación de roles y responsabilidades del personal, los cuales se deben cumplir y respetar.
- Designar a un miembro del área de TI como punto de contacto para comunicar requerimientos de la organización al trabajar con colaboradores, socios, organizaciones de terceros y servicios externos.
- Documentar formalmente planes y procedimientos para monitorear el acceso físico al edificio y la oficina de la empresa
- Monitorear el acceso físico mediante el uso de credenciales que permiten controlar, limitar, monitorear y auditar el acceso a distintas áreas en las oficinas.
- Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware.
- Mantener registros de mantenimiento para documentar reparaciones y modificaciones al software.
- Asignar a una persona encargada de monitorear cualquier actividad inusual quien además deberá investigar a fondo esta actividad y redactar un reporte en caso de que ocurra un incidente sospechoso.
- Definir políticas en caso de falla de algún equipo clave para que siempre se cuente con un equipo respaldo para que el usuario afectado retome sus actividades en el menor tiempo posible.
- Planificar mantenimiento periódico del servidor donde se encuentra alojado el Portal de Gerencia, esto debe estar documentado formalmente y se debe definir un encargado de realizar esta actividad.
- Definir y actualizar periódicamente un inventario de las estaciones de trabajo y equipos con los que cuenta la empresa, para tener control del estado de los mismos.
- Implementar un mecanismo de vigilancia mediante el uso de cámaras para controlar el acceso de personas no autorizadas a las oficinas.

- Establecer políticas para el servidor principal de la organización para que ninguna persona pueda instalar software de tal manera, el único autorizado a hacer instalaciones en los equipos de trabajo es el administrador de la red.
- Incorporar paquetes de actualizaciones a través de la consola del servidor principal para que en la noche los equipos de trabajo se enciendan automáticamente mediante el uso de Wake On LAN y se distribuyan paquetes de actualización de software, antivirus, malware, etc. y se asegure que todos los equipos tengan las mismas y últimas versiones del software actualizado.
- Contratar un seguro para las estaciones de trabajo y equipos de la empresa.
- Documentar formalmente la estrategia que se va a utilizar para controlar el acceso y la autenticación de usuarios ya sea mediante una contraseña que debe ser cambiada periódicamente, tarjetas de identidad inteligentes o un sistema basado en una característica física del usuario.
- Capacitar al personal para que tomen medidas básicas de seguridad para minimizar el acceso no autorizado a sus equipos.
- Asignar responsables encargados de implementar y documentar control de acceso y autenticación de usuarios.
- Cambiar la configuración de autenticación de usuarios y definir qué persona que pertenece a la organización debe tener acceso a cierta información.
- Revisar las estaciones de trabajo para asegurarse que el acceso a las mismas hibernen automáticamente después de un cierto tiempo y pidan ingresar la contraseña.
- Incluir información sobre políticas y procedimientos en el entrenamiento de seguridad.
- Establecer políticas y procedimientos para la planificación de respaldos periódicos de toda la información sensible que se maneja por los usuarios.
- Asegurarse que le personal conozca los nuevos procedimientos de seguridad, esto se puede realizar mediante el envío de correos al personal recordándoles políticas básicas de seguridad.

- Definir planes de recuperación de desastres y continuidad del negocio que permitan garantizar que la organización continuará con sus funciones críticas en caso de haber sido interrumpidas parcial o totalmente.
- Asignar a miembros del personal quienes asistirán a un entrenamiento sobre restricción de usuarios al acceso de información, sistemas susceptibles, servicios específicos, monitoreo del acceso físico, áreas de trabajo, hardware y software.

Finalmente agradezco la apertura y colaboración del personal para con este trabajo y estoy convencida que ha sido un apoyo a su gestión y al desarrollo de su organización en corto, mediano y largo plazo.

4.3 Elaboración del Informe Ejecutivo

Quito, septiembre del 2013

Señor Ingeniero

Pablo Páez, PhD

Gerente General

Pirámide Digital. Cía. Ltda.

De mis consideraciones:

Por medio del presente agradezco la apertura que usted me ofreció tanto a las instalaciones de Pirámide Digital como a la información que se necesitaba para la elaboración del presente proyecto de investigación. Entiendo el enorme esfuerzo que usted ha realizado en Pirámide Digital y espero que el presente proyecto de investigación sea de su utilidad y beneficio en el futuro.

Para realizar la evaluación de riesgo y seguridad utilizando el enfoque que propone OCTAVE-S se utilizaron tres fases: en la fase uno se construyó un perfil de amenaza basado en los activos de la empresa, la fase dos sirvió para identificar vulnerabilidades de la infraestructura y en la fase tres se desarrollaron planes y estrategias de seguridad.

Después de realizar la evaluación utilizando la metodología de OCTAVE-S, se concluye:

- Contar con un programa de entrenamiento sobre conocimiento de seguridad para todo el personal.
- Definir políticas para determinar roles y responsabilidades del personal.
- Documentar planes y procedimientos para monitoreo del acceso físico y autenticación de usuarios.
- Asegurarse que el personal conozca los procedimientos de seguridad.
- Después de terminar con la evaluación, se concluye que la metodología que propone Octave es la mejor entre las opciones existentes ya que es flexible, cubre muchos ámbitos

y permite trabajar directamente con el personal de la organización para asegurarse que los datos recolectados sean lo más acertados.

- Hubo un excelente proceso de aprendizaje para todo el personal involucrado.

A más de presentarle el informe ejecutivo, me comprometo a aclarar cualquier duda o a ampliar cualquier información que no se encuentre totalmente sustentada.

Le reitero, que la información que se presenta a continuación estará únicamente disponible para la empresa y no será divulgada a ninguna persona bajo ninguna circunstancia.

Muchas gracias por su atención y tiempo.

CAPITULO CINCO

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. El trabajo realizado ha sido un gran proceso de aprendizaje para la empresa Pirámide Digital, su Gerente General y para mí; ya que el haber emprendido en esta experiencia que al principio parecía un trabajo sencillo, se transformó en una metodología organizada realizada a través de una serie de tareas que planeadas, ejecutadas y transformadas en realidad sirven para minimizar los riesgos dentro de la organización.
2. Se seleccionó COBIT 4.1 para realizar un análisis de la situación actual de la empresa ya que es un marco de trabajo actualizado, autorizado, fácil de utilizar diariamente y aceptado internacionalmente, el que se puede orientar a todos los sectores de una organización y sirve para auditar la gestión de control de los sistemas de información.
3. Si bien se evaluó COBIT 4.1, ISO 17799 y OCTAVE-S para realizar un análisis de riesgos en la organización, la utilización de OCTAVE-S, viendo hacia atrás, fue la más acertada decisión considerando el tamaño de la empresa, el número del personal, el trabajo que desempeñan y el tipo de negocios que desarrollan.
4. El proceso de aprendizaje dada la estructura de OCTAVE-S fue de fácil aplicación una vez que se tuvo en claro las diferentes fases de la metodología, los procesos que se desarrollan en cada fase y las distintas hojas de trabajo para recolectar información de cada proceso.
5. El equipo de Pirámide Digital con el que estuve involucrada durante la evaluación de OCTAVE-S recibió de una forma receptiva la información y absorbió de manera positiva todo lo planteado lo que hizo que esta experiencia fuera fácil.
6. La metodología para realizar una evaluación de riesgos propuesta por OCTAVE-S es amplia ya que involucra durante toda la evaluación a personal de los altos directivos, directivos de áreas operativas y personal en general, lo que conlleva a que la perspectiva para analizar cada proceso en cada fase sea amplia.

7. En función de la experiencia obtenida por parte de la empresa, se ha pensado incorporar a OCTAVE-S como uno de sus servicios en su cartera de productos que ofrecen a sus clientes dado que esta metodología no es conocida ni explotada en el mercado.
8. Al terminar con la evaluación se presentó al Gerente General un plan de mitigación de riesgos, obteniendo una buena respuesta de las partes.
9. El enfoque presentado en este proyecto de investigación, es un proceso que se puede replicar en cualquier otra empresa de similares características.

5.2 Recomendaciones

1. Pirámide Digital debe revisar el plan de mitigación presentado periódicamente ya que a medida que la tecnología avanza, también crecen las amenazas y riesgos que deben ser considerados para evitar problemas en el futuro.
2. Realizar una nueva evaluación de riesgos utilizando OCTAVE-S cada tres años.
3. Se debe hacer conocer a todo el personal de la organización el plan de mitigación y los siguientes pasos que se recomiendan en esta evaluación.
4. Todo el personal debe asistir a cursos sobre seguridad de tal manera que todos tengan conocimiento y sepan cómo actuar en caso de que se presente una amenaza a cualquier activo crítico de la empresa.
5. Utilizar el proceso desarrollado en este plan de disertación para realizar una evaluación de riesgos y seguridad para otras actividades y situaciones en otra empresa.
6. Evaluar otros activos críticos.
7. A la facultad, considero es importante se considere en el pensum de la carrera incorporar una materia en la que se explique qué es la evaluación de riesgos.

BIBLIOGRAFÍA

[1] J. Lozano, «Seguridad de la Información. Riesgos,» [En línea]. Available: www.elmayorportaldegerencia.com/documentos/188-tecnologias-de-informacion-y-comunicacion. [Último acceso: 27 diciembre 2012].

[2] C. Alberts, «Introduction to the Octave approach,» [En línea]. Available: www.itgovernanceusa.com/files/ Octave.pdf . [Último acceso: 10 enero 2013].

[3] C. P. Woody, «Applying Octave: Practitioners report,» CMU/SEI-2006-TN-010, Pittsburg, PA, 2006.

[4] C. Alberts, Managing Information Security Risks: The Octave Approach, Estados Unidos: Addison-Wesley Professional, 2002, pp. 123-127.

[5] A. Dorofee, «Asset-Based information security risk assessments, Cutter Consortium, Enterprise Risk Management and Governance Executive Report,» Arlington MA, 2009.

[6] C. Alberts, Managing Information Security Risks: The Octave Approach, Estados Unidos: Wesley Professional, 2002, p. 118.

[7] D. Bieber, «The critical success factor method,» [En línea]. Available: www.cert.org/archive/pdf/04tr010.pdf. [Último acceso: 24 enero 2013].

[8] J. Lozano, «Seguridad de la Información,» [En línea]. Available: . www.elmayorportaldegerencia.com/ documentos/188-tecnologias-de-informacion-y-comunicación. [Último acceso: 27 diciembre 2012].

[9] J. Lozano, «Seguridad de la Información. Riesgos segunda parte,» [En línea]. Available: www.elmayorportaldegerencia.com/ documentos/188-tecnologias-de-informacion-y-comunicación. [Último acceso: 27 diciembre 2012].

[10] E. Rosero, «Introducción a la seguridad de la información,» [En línea]. Available: www.elmayorportaldegerencia.com/index.php/documentos/188-tecnologias-de-informacion-y-comunicacion/ . [Último acceso: 20 enero 2013].

[11] C. Alberts, Managing Information Security Risks: The Octave Approach, Estados Unidos: Wesley Professional, 2002, p. 5.

[12] C. Alberts, «Security Risk Analysis with Octave,» [En línea]. Available: Internet. www.informit.com/articles/. [Último acceso: 25 enero 2013].

[13] P. Cevallos, «Introducción a defensa en profundidad y seguridad de la información TI,» [En línea]. Available: www.repositorio.utn.edu.ec. [Último acceso: 27 enero 2013].

[14] N. Guayaquil, *Estándar ISO 1779 y Norma ISO 27001*, Quito, 2007, pp. 3-31.

[15] J. Mc Leod, «Octave method,» [En línea]. Available: www.cert.org/octave. [Último acceso: 27 enero 2013].

[16] R. Arbeláez, «Modelos de madurez de seguridad de la información: cómo debe evolucionar la seguridad en las organizaciones,» [En línea]. Available: www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/05-ModelosMadurezSeguridadInformatica.pdf. [Último acceso: 11 febrero 2013].

[17] M. Adler, Manual Cobit 4.1 en español, Rolling Meadows, 2007.

[18] C. Alberts, OCTAVE-S Implementation Guide: Example Scenario, vol. 10, Pittsburgh, PA, 2005.

ANEXO A: MATRICES DE MADUREZ DE COBIT

Proceso PO1: Definición de un plan estratégico de tecnología de TI

Dominio: Planeación y Organización					
Proceso: PO1 – Definición de un plan estratégico de tecnología de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La alta gerencia desconoce la necesidad de planeación estratégica?				
	¿La alta gerencia apoya el plan estratégico?				
	¿Existe una estructura de planeación?				
	¿La planeación apoya a las metas?				
	¿Se desconoce la existencia de planeación?				
1	¿La planificación estratégica es conocida por la gerencia TI?				
	¿La planificación estratégica se elabora por un requisito comercial específico?				
	¿La planificación de la empresa es discutida ocasionalmente en las reuniones de administración?				
	¿La posición de riesgo estratégica está identificada informalmente en base a los proyectos?				
	¿La planificación estratégica evoluciona constantemente de acuerdo a las necesidades de la empresa?				
2	¿El plan estratégico está entendido sustancialmente por la gerencia?				
	¿La planificación estratégica se comparte ocasionalmente con la gerencia de ventas?				
	¿El plan estratégico ocurre en respuesta a las demandas administrativas?				
	¿Hay procesos para identificar actualizaciones del plan?				

	¿Dentro de la empresa los procesos de planificación estratégica son claros y concisos?				
3	¿Están definidas las políticas que define cuando y como se realiza la planificación estratégica?				
	¿La planificación estratégica involucra a todo el personal?				
	¿Existe algún procedimiento para examinar el proceso en una base regular?				
	¿La estrategia global TI incluye una definición global de riesgos?				
	¿Las estrategias de los recursos financieros incluyen a todos los ámbitos de la empresa?				
4	¿La planificación estratégica tiene la supervisión de la dirección?				
	¿La planificación estratégica está definida con mayores responsabilidades niveladas?				
	¿La planificación estratégica establece las prácticas estándar y sus excepciones son notadas por la dirección?				
	¿Existe un proceso bien definido para equilibrar los recursos necesarios para el desarrollo y funcionamiento de la empresa?				
	¿Existe una función de administración definida con mayores responsabilidades niveladas?				
5	¿El plan estratégico está considerado dentro de los objetivos comerciales de la empresa?				
	¿Existe una función de la planificación estratégica que está integrada con la planificación comercial?				
	¿El plan estratégico está diseñado para ser implementado a largo plazo?				

	¿El plan estratégico es versátil?				
	¿El plan estratégico está diseñado respetando las normas que rigen la empresa?				

Proceso PO3: Determinar la dirección tecnológica

Dominio: Planeación y Organización					
Proceso: PO3 – Determinar la dirección tecnológica					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa pone interés en planear la infraestructura tecnológica?				
	¿Existe un plan de infraestructura?				
	¿Hay experiencia y conocimiento para realizar un plan de infraestructura documentado y formal?				
	¿Existe personal capacitado en su organización que tenga las habilidades y conocimientos para realizar un plan de infraestructura?				
	¿Se entiende la importancia de planear un cambio para focalizar correctamente los recursos?				
1	¿Los directivos reconocen la necesidad de un plan pero no lo tienen aún?				
	¿El desarrollo de tecnología está muy limitado?				
	¿Los directivos enfocan su atención en la necesidad de realizar planeación?				
	¿La dirección de la tecnología del negocio está a cargo de vendedores o personas incorrectas?				
	¿La comunicación es inconsistente sobre el impacto en cambios de tecnología?				
2	¿Se comunica la necesidad y la importancia de realizar un plan tecnológico?				
	¿La planeación se enfoca en solucionar problemas técnicos en vez de cumplir las necesidades del negocio?				

	¿La evaluación de cambios tecnológicos está a cargo de diferentes individuos que siguen procesos similares?				
	¿Existe un entrenamiento formal y comunicación de los roles y responsabilidades?				
	¿Se reconoce en su organización que están apareciendo técnicas y estándares comunes para el desarrollo de la infraestructura?				
3	¿Los directivos conocen sobre el plan de infraestructura tecnológica?				
	¿El plan estratégico de TI está alineado con el plan de infraestructura tecnológica?				
	¿Se creó un plan de infraestructura tecnológica definido, documentado y bien comunicado pero inconsistente para su aplicación?				
	¿Los empleados y directivos entienden a donde se dirige la organización considerando riesgos y alineado con el plan estratégico?				
	¿Se seleccionan los mejores vendedores considerando su experiencia y conocimiento para la compra de tecnología?				
4	¿El plan estratégico de infraestructura tecnológica fue creado por gente con experiencia?				
	¿Se capacita de manera formal y especializada a los nuevos empleados para que conozcan el plan estratégico de la empresa?				
	¿Se tiene en cuenta el impacto del cambio de tecnología?				
	¿Se anticipa a los problemas y se asignan responsables para cumplir y actualizar el plan de infraestructura tecnológica?				

	¿Se introducen las mejores prácticas internas en los procesos?				
5	¿Se dirige la empresa utilizando estándares de la industria?				
	¿Se administra con alto nivel los impactos que los cambios de tecnología generan?				
	¿Se aprueba de manera ejecutiva el cambio de tecnología?				
	¿Está formalizada la participación en estándares?				
	¿Se utiliza de manera exhaustiva las mejores prácticas de la industria?				

Proceso PO4: Definir procesos, organización y relaciones de TI

Dominio: Planeación y Organización					
Proceso: PO4 – Definir procesos, organización y relaciones de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización de TI se centra efectivamente a enfocar el logro de los objetivos del negocio?				
1	¿Las actividades y funciones de TI están implementadas, pero son inconsistentes?				
	¿Se ha definido una estructura organizacional, roles y responsabilidades que están informalmente asignadas?				
	¿La función de TI se considera una función de soporte que no incluye en su totalidad la perspectiva de organización?				
2	¿Existe un entendimiento implícito acerca de la necesidad de implementar una organización de TI?				
	¿Roles y responsabilidades no están formalizados o no se cumplen?				
	¿La función de la TI está organizada para responder tácticamente, pero inconsistentemente?				
	¿La necesidad para una organización estructurada y de administración está vilmente comunicada, pero las decisiones que se toman son dependientes del conocimiento y de las herramientas claves de uso individual?				
	¿Existen técnicas emergentes comunes para administrar la organización de TI y sus relaciones?				
3	¿Se han definido roles y responsabilidades para la organización de la TI y de terceros?				
	¿La organización de la TI está desarrollada, documentada, comunicada y alineada con la estrategia				

	de TI?				
	¿El diseño organizacional y el control interno del entorno están definidos?				
	¿Hay formalización de relaciones con otras partes interesadas?				
	¿La organización de TI está funcionalmente completa?				
4	¿El personal de la TI tiene la experiencia y formación necesaria para desarrollar un plan de infraestructura de tecnología?				
	¿Existe un formal y especializado entrenamiento para la investigación de la tecnología?				
	¿La responsabilidad para el desarrollo y mantenimiento de un plan de infraestructura de tecnología podría ser asignada?				
	¿La estrategia de los recursos humanos está alineada con la dirección de la tecnología para asegurar que el personal de la TI pueda manejar los cambios de la tecnología?				
	¿La dirección de TI está guiada por la industria y estándares internacionales y de desarrollo?				
5	¿Existe aprobación ejecutiva formal de un nuevo cambio de reglas tecnológicas?				
	¿La entidad tiene un plan de infraestructura robusta que refleje los requerimientos del negocio?				
	¿Existe una continua y real mejora de los procesos en el ambiente de trabajo?				
	¿Las mejores prácticas de la industria están extensivamente usadas en determinadas reglas de la técnica de las TI's?				

Proceso PO9: Evaluar y administrar riesgos de TI

Dominio: Planeación y Organización					
Proceso: PO9 – Evaluar y administrar riesgos de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Se realiza un análisis sobre el riesgo de imposición de contribuciones para procesos y decisiones del negocio?				
1	¿La organización considera los impactos de negocio asociados con vulnerabilidades de seguridad y con desarrollo de proyectos inciertos?				
	¿El manejo de riesgos se ha visto identificado como relevante para adquirir soluciones de TI y deliberadamente servicios de TI?				
	¿La organización sabe de sus responsabilidades tanto legal como contractual y riesgos, considerándolos en una manera ad hoc?				
	¿El manejo de TI especifica las responsabilidades para el manejo de riesgos en descripciones de trabajo u otros significados informales?				
	¿La especificación de TI relaciona riesgos tales como seguridad e integridad y son ocasionalmente considerados en un proyecto como base principal del mismo?				
2	¿Los riesgos de TI relacionados día a día a las diferentes operaciones de la TI son infrecuentemente discutidos en las reuniones de la AG?				
	¿Los riesgos consideran que la mitigación o calma es inconsistente dentro del área de TI?				
	¿Existe un deseo emergente de entender que los riesgos de TI son importantes y necesarios para ser				

	considerados?				
	¿Hay algún acercamiento al riesgo de distribución de contribuciones existentes, dentro del área de TI?				
3	¿El área de TI define generalmente procedimientos o descripciones de trabajo gestionando con la Gerencia de TI?				
	¿La distribución de contribuciones en las diferentes operaciones de TI depende mediáticamente de un manejo creciente, por lo que esta tiene una gran importancia dentro de la agenda de trabajo?				
	¿El riesgo de distribución de contribuciones sigue un proceso definido que es documentado y reconocido por todo el personal a través del entrenamiento?				
	¿Las decisiones que se toman a consideración por la AG son salidas efectivas a una posible crisis dentro de la TI?				
	¿La metodología es convincente y segura?				
4	¿Todos los proyectos que fueron cubiertos o están en operación son examinados sobre una base de riesgos?				
	¿El manejo de la política de una organización grande define cuándo y cómo debe conducirse los riesgos de distribución de contribuciones?				
	¿La distribución de contribuciones de riesgo es un procedimiento y excepciones a seguir por la AG?				
	¿El manejo de los riegos de TI está definido en función con el nivel de responsabilidad de la AG?				
	¿La AG es notificada de los cambios en el entorno de la TI lo cual puede significativamente afectar al escenario de riegos?				
5	¿La AG es capaz de monitorear la posición de riesgo y adoptar una decisión acertada que sea acogida por el				

	personal de la TI?				
	¿El manejo efectivo de una base de datos de riegos está debidamente establecido?				
	¿La distribución de contribuciones habría de desarrollar una organización la cual siga regularmente el buen manejo de su estructura?				
	¿El análisis y reporte de riegos son altamente automatizados?				
	¿El manejo de riegos es verdaderamente aceptable y extensible para los miembros de la USI?				

Proceso AI5: Instalar y acreditar sistemas

Dominio: Adquisición e Implementación					
Proceso: AI5 – Instalar y acreditar sistemas					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa tiene un proceso formal de instalación de nuevas tecnologías tanto de hardware como de software?				
	¿La empresa posee un proceso formal que verifica que la solución sea adecuada y esté alineada con los objetivos de TI?				
	¿El personal reconoce la necesidad de verificar si las soluciones que se dan encajan con el propósito deseado?				
1	¿La empresa reconoce la necesidad de verificar y confirmar que las soluciones que se implementen contribuyen al propósito deseado?				
	¿La empresa realiza pruebas para algunos proyectos?				
	¿La empresa depende de iniciativas del equipo del proyecto para realizar las pruebas?				
	¿Los resultados que obtiene la empresa al realizar las pruebas usualmente varían?				
	¿La empresa tiene una acreditación formal y estar fuera de línea es esporádico o inexistente?				
2	¿La empresa tiene alguna consistencia entre la comprobación y la acreditación?				
	¿La empresa basa sus pruebas en metodologías?				
	¿Existe normalmente una ausencia de comprobación de la integración?				
	¿Existe cierto proceso de la aprobación informal, no necesariamente basado en un criterio regularizado?				

	¿Existe una acreditación formal y estar fuera de línea es aplicado incoherentemente?				
3	¿Está implementada una metodología formal relacionada con la instalación, migración, conversión y existe una aceptación?				
	¿Existe la habilidad de mantener un cumplimiento en la administración?				
	¿Se encuentran integrados y de alguna forma automatizados los procesos de Instalación y acreditación de TI dentro del ciclo de vida del sistema?				
	¿Los entrenamientos, pruebas y la transición entre el estado de producción y acreditación varían de los procesos definidos, y se basan en decisiones individuales?				
	¿Es inconsistente la calidad de los sistemas que ingresan a la etapa de producción, generando así problemas de post-implementación?				
4	¿Los procesos se encuentran formalizados y desarrollados para encontrarse bien organizados y ser prácticos, con ambientes de prueba y procesos de acreditación definidos?				
	¿La evaluación para alcanzar los requerimientos de usuario está estandarizada y puede ser medida?				
	¿La calidad de los sistemas que ingresan a la etapa de producción es satisfactoria para la administración?				
	¿Se emplean evaluaciones post-implementación ni revisiones continuas de calidad?				
	¿El sistema de pruebas refleja de forma adecuada el ambiente real?				

5	¿Los procesos de instalación y acreditación se encuentran refinados a un nivel de las mejores prácticas, basados en una continua mejora y refinamiento?				
	¿Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y automatizados?				
	¿Se disponen de ambientes de prueba bien desarrollados y los procesos de registro de problemas y fallas aseguran una transición de eficiencia y efectividad hacia el ambiente de producción?				
	¿La acreditación se da con una mínima necesidad de reformularla y los problemas post-implementación son correcciones menores?				
	¿Las revisiones de post-implementación son estandarizadas y son retroalimentadas hacia los procesos para asegurar una continua mejora en cuanto a la calidad?				

Proceso AI6: Administrar cambios

Dominio: Adquisición e Implementación					
Proceso: AI6 – Administrar cambios					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Existe un proceso definido de administración de cambio y estos cambios se pueden realizar virtualmente sin control?				
1	¿Existen políticas de administración y control de cambios tecnológicos en la organización?				
	¿Se sigue algún proceso consistente a seguir para el control de cambios tecnológicos?				
	¿Cambia continuamente el proceso de cambios tecnológicos en la organización?				
	¿Se requiere de autorización superior para ejecutar cambios de tecnología?				
	¿Cuándo un cambio de tecnología se ejecuta en la organización, es necesario documentar el mismo?				
2	¿Existe un proceso formal definido para el proceso de administración y control de los cambios?				
	De existir este proceso, ¿está estructurado formalmente?				
	¿Considera que la documentación de configuración es precisa y consistente?				
	¿Considera que las tareas de planeamiento e impacto son prioritarias a los cambios?				
	¿Existe frecuentemente un re-doble de trabajo, en tareas ya efectuadas?				
	¿Existe un proceso formalmente definido para la administración de cambios?				
	¿El proceso de administración de cambios incluye				

3	priorización, categorización, control de contingencias, autorización de cambios y administración de lanzamientos?				
	¿Considera que el proceso de administración de cambios es siempre práctico y aplicable?				
	¿Ocurren cambios sin autorización ocasionalmente?				
	¿Existe un análisis operacional del impacto que causan los cambios tecnología en el negocio?				
4	¿Se sigue de forma consistente el proceso de administración de cambios, confía que en el mismo no hay excepciones?				
	¿El proceso de administración de cambios mantiene procesos y controles manuales para asegurar calidad?				
	¿Están sujetos los cambios a reducir la posibilidad de problemas post-producción, a través de las tareas de planificación e impacto?				
	¿Considera que las tareas planeamiento e impacto son prioritarias a los cambios?				
	¿El monitoreo de cambios es un proceso formal dentro de los documentos de administración de cambios?				
5	¿Se actualiza regularmente el proceso de administración de cambios?				
	¿El proceso de administración de cambios cambia de acuerdo a la línea de las "mejores prácticas"?				
	¿La información de configuración se encuentra implementada en una aplicación para controlar la misma?				
	¿El monitoreo de la configuración y de la administración de lanzamientos, incluye herramientas para la detección de software sin licencia o sin				

	autorización?				
	¿La administración de cambios tecnológicos está integrada a los cambios del negocio?				

Proceso DS1: Definir y administrar niveles de servicio

Dominio: Entrega y Soporte					
Proceso: DS1 – Definir y administrar niveles de servicio					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La administración ha reconocido la necesidad de un proceso para definir niveles de servicio?				
	¿Están asignados responsables cuando existen problemas en los procesos?				
	¿Están asignadas las responsabilidades para la administración de servicios?				
	¿Están definidos los niveles de servicio?				
	¿La administración conoce sobre las obligaciones y responsabilidades que tiene en cuanto a niveles de servicio?				
1	¿Existe conciencia de la necesidad de administrar niveles de servicio?				
	¿El proceso para la administración de Niveles de Servicio es informal?				
	¿Está definida informalmente la rendición de cuentas del desempeño de monitoreo?				
	¿Las mediciones del desempeño son cualitativas?				
	¿El reporte del desempeño es frecuente?				
2	¿Existen acuerdos celebrados sobre el nivel de servicio?				
	¿El reporte de nivel de servicio es relevante y completo?				
	¿El reporte de nivel de servicio depende de las habilidades de los administradores individuales?				
	¿Se debería nombrar un coordinador de nivel de servicio?				

	¿El proceso de cumplimiento del acuerdo de nivel de servicio es voluntario?				
3	¿Están bien definidas las responsabilidades de la administración de nivel de servicio?				
	¿El proceso de desarrollo de los acuerdos de nivel de servicio está establecido con puntos de verificación?				
	¿Están definidos con los usuarios los criterios de niveles de servicios?				
	¿Están identificadas las carencias de nivel de servicio?				
	¿El nivel de servicio puede resolver las necesidades específicas de la organización?				
4	¿La satisfacción del cliente se determina de manera rutinaria?				
	¿Las medidas de desempeño reflejan las metas de TI?				
	¿Están estandarizados los criterios de medición de los niveles de servicio?				
	¿Se realiza un análisis de causas originarias?				
	¿Están entendidos con claridad los riesgos operativos?				
5	¿Los niveles de servicio son reevaluados constantemente?				
	¿Todos los procesos de nivel de servicio están sujetos a procesos de mejoramiento?				
	¿Un criterio para definir niveles de servicio es basarse en la criticidad del negocio?				
	¿Los niveles de satisfacción del cliente son monitoreados?				
	¿Los niveles de servicio esperados son evaluados contra las normas de la industria?				

Proceso DS5: Garantizar la seguridad de los sistemas

Dominio: Entrega y Soporte					
Proceso: DS5 – Garantizar la seguridad de los sistemas					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La empresa reconoce la necesidad de seguridad para el área de TI?				
	¿Se asignan responsabilidades para encargarse de la seguridad?				
	¿Existe la implementación de medidas que soporten la administración de TI?				
	¿La empresa posee un proceso de administración para la seguridad de TI?				
	¿Existen procesos de reportes y soluciones para problemas de seguridad en TI?				
1	¿La empresa reconoce la necesidad de la seguridad en TI?				
	¿La seguridad es administrada según criterios del individuo responsable?				
	¿Las responsabilidades para la administración de seguridad en TI son confusas?				
	¿Hay una persona responsable para la administración de problemas de seguridad?				
	¿Las soluciones para problemas de seguridad son previsibles?				
2	¿Las responsabilidades de seguridad de TI son asignadas a un coordinador de seguridad sin autoridad de gerencia?				
	¿El reporte de la seguridad es pertinente?				
	¿El conocimiento acerca de la seguridad es fragmentado y limitado?				

	¿La información de la seguridad es generada pero no analizada?				
	¿Las políticas de seguridad están siendo desarrolladas pero se utilizan técnicas y herramientas inadecuadas?				
3	¿La Empresa promueve el conocimiento acerca de la seguridad?				
	¿Los informes de la seguridad se han formalizado y se han estandarizado?				
	¿Los procesos de seguridad de TI están definidos y es complemento de la estructura de políticas y procedimientos de seguridad?				
	¿Las responsabilidades para la seguridad de TI son asignadas pero no consistentemente cumplidas?				
	¿Existe un plan de seguridad conduciendo a análisis de riesgo y soluciones de seguridad?				
4	¿Las responsabilidades para la seguridad de TI son claramente asignadas, administradas y ejecutadas?				
	¿Las políticas y prácticas de seguridad son completas, con específicas y bases de seguridad?				
	¿Los informes sobre la seguridad de TI se han convertido en una obligación?				
	¿La Empresa establece la certificación de seguridad en el personal?				
	¿Los procesos de la seguridad de TI son coordinados con la función global de seguridad de la empresa?				
5	¿Los requerimientos de seguridad de TI están claramente definidos, optimizados e incluidos en el plan de seguridad?				
	¿Los incidentes de seguridad de TI son tratados puntualmente con los procedimientos formalizados soportados por herramientas automatizadas?				

	¿Los procesos de seguridad y tecnologías están integrados totalmente a la empresa?				
	¿Las funciones de seguridad se integran con las aplicaciones en la etapa de diseño?				
	¿Las pruebas de intrusión, análisis de causalidad y la identificación de riesgos no están perfectamente implementadas?				

.

Proceso DS10: Administrar los datos

Dominio: Entrega y Soporte					
Proceso: DS10 – Administrar los datos					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿Hay conciencia de la necesidad de administrar problemas e incidentes?				
	¿El proceso de resolución de problemas es informal?				
	¿Los usuarios y el personal de TI resuelven los problemas de manera individual?				
	¿Los problemas se resuelven caso por caso?				
	¿Existen procesos para el manejo de incidentes?				
1	¿La organización ha reconocido que hay una necesidad de resolver problemas y de evaluar los incidentes?				
	¿Las personas con conocimientos clave proveen alguna asistencia con los problemas relacionados con su área de experiencia y responsabilidad?				
	¿La información es compartida con otros y las soluciones varían de una persona de soporte a otra?				
	¿Con medidas equivocadas se da la creación de más problemas y la pérdida de tiempo productivo, mientras se buscan las respuestas?				
	¿La administración cambia frecuentemente el enfoque y la dirección de las operaciones y el personal de soporte técnico?				
2	¿Hay una amplia conciencia de la necesidad de administrar los problemas e incidentes relacionados con TI?				
	¿El proceso de resolución ha evolucionado hasta un				

	grado en que unas pocas personas claves son responsables de administrar los problemas e incidentes que ocurren?				
	¿La información es compartida entre el personal; sin embargo, el proceso sigue sin estructuración, es informal y mayormente reactivo?				
	¿El nivel de servicio para la comunidad de usuarios varía y es obstaculizado por insuficientes conocimientos estructurados disponibles para quienes resuelven los problemas?				
	¿El reporte de la administración de incidentes y el análisis de la creación de problemas es limitado e informal?				
3	¿La necesidad de un sistema efectivo de administración de problemas es aceptada y evidenciada por presupuestos para la contratación de personal?				
	¿Los procesos de resolución, escalamiento y resolución de problemas han sido estandarizados, pero no son sofisticados?				
	¿Los usuarios han recibido comunicaciones claras sobre dónde y cómo reportar sobre problemas e incidentes?				
	¿El registro y rastreo de problemas y sus resoluciones es fragmentado dentro del equipo de respuestas, usando las herramientas disponibles sin centralización o análisis?				
	¿Es probable que las desviaciones de las normas o estándares establecidos pasen desapercibidas?				
4	¿El proceso de administración de problemas es				

	entendido en todos los niveles dentro de la organización?				
	¿Las responsabilidades son claras y establecidas?				
	¿Los métodos y procedimientos están documentados, comunicados y medidos por efectividad?				
	¿La mayoría de los problemas e incidentes están identificados, registrados, reportados y analizados en busca de constante mejoramiento y son reportados a las partes interesadas?				
	¿La capacidad de responder a los incidentes es probada periódicamente?				
5	¿El proceso de administración de problemas ha evolucionado en un proceso que mira hacia adelante y es proactivo, contribuyendo a los objetivos de TI?				
	¿Los problemas son anticipados y pueden incluso ser prevenidos?				
	¿El conocimiento es mantenido, a través de contactos regulares con vendedores y expertos, respecto de patrones de problemas e incidentes pasados y futuros?				
	¿El registro, reporte y análisis de problemas y resoluciones es automatizado y está totalmente integrada con la administración de configuración de datos?				
	¿La mayoría de los sistemas han sido equipados con mecanismos automáticos de detección y de advertencia, que son constantemente rastreados y evaluados?				

Proceso ME1: Monitorear el desempeño de TI

Dominio: Monitoreo y Evaluación					
Proceso: ME1 – Monitorear el desempeño de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización cuenta con un proceso de monitoreo?				
	¿El área de TI desarrolla independientemente un monitoreo de proyectos o procesos?				
	¿Se reconoce la necesidad de objetivos de procesos claramente entendibles?				
1	¿Se reconoce la necesidad de colectar y determinar información acerca de procesos de monitoreo?				
	¿Se han identificado procesos determinados y una colección estándar?				
	¿Se implementa un monitoreo constante solamente cuando un incidente causa alguna perdida a la organización?				
	¿Se implementa el monitoreo para los procesos de TI y tan solo para servicios de información de otros departamentos?				
	¿La definición del proceso y el monitoreo se ajustan a las necesidades de los servicios de información?				
2	¿Han sido identificadas algunos parámetros para monitorear?				
	¿Se ha adoptado una colección de métodos y técnicas, pero no por toda la organización?				
	¿La planeación y administración es realizada por el expertise de individuos claves?				
	¿Algunas herramientas son implementadas y usadas pero se limita el uso por falta del expertise en el				

	manejo?				
	¿La función de servicios de información es manejada como un centro que genera costos y no beneficia a la organización?				
3	¿La administración ha institucionalizado y comunicado los estándares para monitorear procesos?				
	¿Un programa de educación y entrenamiento para monitorear ha sido implementado?				
	¿Han sido implementadas herramientas para monitorear el nivel de servicio y procesos de TI?				
	¿Han sido definidos parámetros para medir la contribución del nivel de servicio en la organización?				
	¿Han sido implementados los parámetros para medir la satisfacción del cliente y del nivel de servicio en las entidades?				
4	¿La gerencia define tolerancias en las cuales los procesos deben operar?				
	¿Lineamientos base de resultados de monitoreo son estandarizados y normalizados?				
	¿Existe integración de las métricas entre proyectos TI y procesos?				
	¿Se define un marco para identificar estrategias orientadas a procesos como KGIs, KPIs, y CSFs para realizar mediciones?				
	¿Se ejecutan criterios de aprendizaje tales como financieros, operacionales, de consumidores y organizacional?				
5	¿Se mejora el proceso para actualizar el monitoreo de estándares, políticas y mejores prácticas en la organización?				
	¿Todos los procesos de monitoreo son optimizados y				

	soportan objetivos globales de la organización?				
	¿KGIs, KPIs, y CSFs son usados continuamente para realizar mediciones y se alinean con el trabajo estratégico?				
	¿Procesos de monitoreo y rediseños en movimiento son consistentes con planes ya desarrollados de mejoramiento?				
	¿Bancos de prueba contra la industria y competidores claves se formalizan y comparan?				

Proceso ME2: Monitorear y evaluar el control interno

Dominio: Monitoreo y Evaluación					
Proceso: ME2 – Monitorear y evaluar el control interno de TI					
Nivel	**Pregunta**	**Si**	**Parcialmente**	**No**	**Análisis**
0	¿La organización posee procedimientos para monitorear la efectividad de los controles internos?				
	¿Los métodos de reporte de control interno de administración están presentes en su organización?				
	¿Hay una ausencia general de conciencia de la seguridad operativa?				
	¿La administración y los empleados tienen conciencia de los controles internos?				
	¿Hay una ausencia general del aseguramiento de control interno de TI?				
1	¿Existe un compromiso de parte de la administración para la seguridad operativa regular?				
	¿Se aplica ad hoc en la experiencia individual en determinar la adecuación de control interno?				
	¿La administración de TI ha asignado formalmente la responsabilidad de monitorear la efectividad de los controles Internos?				
	¿Las evaluaciones de control interno de TI son realizadas como parte de auditorías financieras tradicionales?				
	¿Existe un monitoreo adecuado dentro de la empresa?				
2	¿La organización usa reportes informales de control para iniciar iniciativas de acción correctiva?				
	¿Los procesos de planificación y administración están definidos?				
	¿La evaluación depende de los conjuntos de				

	habilidades de las personas clave?				
	¿La organización tiene una mayor conciencia del monitoreo de control interno?				
	¿La administración ha comenzado a establecer métricas básicas?				
3	¿La administración soporta y ha institucionalizado un monitoreo de control interno?				
	¿Se han desarrollado políticas y procedimientos para evaluar y reportar sobre las actividades de control interno?				
	¿No se ha establecido una base de conocimientos de métrica para información histórica sobre el monitoreo de control interno?				
	¿No se ha implementado un programa de educación y entrenamiento para el monitoreo de control interno?				
	¿Se han establecidos revisiones periódicas para el monitoreo del control Interno?				
4	¿La administración ha establecido Benchmarking y metas cuantitativas para los procesos de revisión del control interno?				
	¿La organización estableció niveles de tolerancia para el proceso de monitoreo de control interno?				
	¿Están incorporadas herramientas integradas y cada vez más automatizadas en los procesos de revisión del control interno?				
	¿Los riesgos específicos del proceso y las políticas de mitigación están definidos para toda la función de servicios de Información?				
	¿Está establecida una función formal de control interno de TI con profesionales?				
5	¿La administración ha establecido un programa de				

	mejoramiento continuo a través de toda la organización?				
	¿La organización usa herramientas avanzadas que son integradas y actualizadas?				
	¿Está formalizada la participación de los conocimientos?				
	¿Están implementados programas formales de entrenamiento específicos para la función de los servicios de información?				
	¿Los marcos de control de TI están integrados con marcos y metodologías a nivel de toda la organización?				

ANEXO B: HOJAS DE TRABAJO OCTAVE-S

Hoja de Trabajo. Impacto de los criterios de la evaluación: Reputación y Confianza del Cliente

Reputación/Confianza del Cliente			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Reputación	La reputación de la empresa se afecta en un mínimo porcentaje, poco o nada de esfuerzo o gasto es necesario para recuperarse si se presenta la situación de pérdida de confianza del cliente.	La reputación de la empresa se daña, y esfuerzo y un poco de gasto económico se requiere para recuperarse.	La reputación de la empresa está irremediablemente destruida o dañada.
Pérdida de clientes	Menos del ____% de reducción de clientes debido a la pérdida de confianza.	Del ____ al ___% de reducción de clientes debido a la pérdida de confianza	Más del ____% de reducción de clientes debido a la pérdida de confianza.
Otro:			

Hoja de Trabajo. Impacto de los criterios de la evaluación: Finanzas

Finanzas			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Costos operativos	Aumento de menos de ____% anual en costos operativos	Gastos anuales de costos operativos aumentan del ____ al ___%	Anualmente los costos operativos aumentan el ____%
Pérdida de ingresos	Menos de ____% de pérdida de ingresos anuales	De ____ al ___% de pérdida de ingresos anuales	Mayor del ____%en pérdida de ingresos anuales
Pérdida financiera	Pérdida financiera de menos de $ ____	Pérdida financiera de $ ____ al $___	Pérdida financiera mayor a $____
Otro:			

Hoja de Trabajo. Impacto de los criterios de la evaluación: Productividad

Productividad			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Horarios del personal	El horario del personal se incrementó menos del ____% en ___ día(s)	El horario del personal se incrementó entre el ____ al ____% en ___ día(s)	El horario del personal se incrementó en más de un ____% en ___ día(s)
Otro:			
Otro:			
Otro:			

Hoja de Trabajo. Impacto de los criterios de la evaluación: Seguridad/Salud

Seguridad/Salud			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Vida	No hay pérdida o amenaza significativa en la vida del personal	La vida de los miembros del personal se ven amenazadas, pero se recuperarán después de recibir tratamiento médico.	Pérdida de vidas de miembros del personal
Salud	Degradación mínima, inmediatamente tratable de la salud de los miembros del personal con un tiempo de recuperación dentro de cuatro días	Discapacidad temporal o recuperable de la salud de miembros del personal	Deterioro permanente de la salud de miembros del personal
Seguridad	Seguridad cuestionada	Seguridad afectada	Seguridad violada
Otro:			

Hoja de Trabajo. Impacto de los criterios de la evaluación: Multas/Sanciones Legales

Multas/Sanciones Legales			
Tipo de Impacto	**Bajo Impacto**	**Mediano Impacto**	**Alto Impacto**
Multas	Multas inferiores a $_____ son recaudadas	Multas entre $_____ y $_____ son recaudadas	Multas mayores a $_____ son recaudadas
Demandas	Demandas no frívolas de menos de $ ____ son presentadas en contra de la organización	Demandas no frívolas entre $_____ y $_____ son presentadas en contra de la organización	Demandas no frívolas mayores a $_____ son presentadas en contra de la organización
Investigaciones	No hay preguntas formuladas por el gobierno u otras organizaciones de investigación	El gobierno u otras organizaciones de investigación requieren información o records de la empresa	El gobierno u otras organizaciones de investigación inician una investigación de alto perfil y en profundidad de las prácticas de la organización
Otro:			

Hoja de Trabajo. Identificación de activos organizacionales: Información, Sistemas y Aplicaciones

Información, Sistemas y Aplicaciones			
Sistema ¿Qué sistemas la gente en su organización necesita para realizar su trabajo?	**Información** ¿Qué información la gente en su organización necesita para realizar su trabajo?	**Aplicaciones y Servicios** ¿Qué aplicaciones y servicios la gente en su organización necesita para realizar su trabajo?	**Otros Activos** ¿Qué otros activos están relacionados directamente con estos activos?

Hoja de Trabajo. Identificación de activos organizacionales: Gente

Gente			
Gente *¿Qué personas tienen una habilidad o conocimiento especial que es vital para su organización y puede ser muy difícil de reemplazar?*	**Habilidades y Conocimiento** *¿Cuáles son sus habilidades o conocimientos?*	**Sistemas Relacionados** *¿Qué sistemas utilizan estas personas?*	**Activos Relacionados** *¿Qué otros activos usan estas personas (Ejemplo: información, servicios o aplicaciones)*

Hoja de Trabajo. Prácticas de seguridad: Seguridad, Concientización y Entrenamiento

Seguridad, Concientización y Entrenamiento				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Los miembros del personal comprendan sus roles de seguridad y responsabilidades. Esto está documentado y verificado.	Si Algo No No se sabe			Rojo Amarillo Verde No aplica
Hay suficiente experiencia interna para todas las versiones servicios, mecanismos y tecnologías. Esto está documentado y verificado.	Si Algo No No se sabe			
Existe una conciencia de seguridad, capacitación y recordatorios periódicos, los que se proporcionan para	Si Algo No No se sabe			

todo el personal. El entendimiento del personal está documentado y se verifica periódicamente.				
Los miembros del personal siguen buenas prácticas como: • Asegurar información de la que son responsable • No divulgar información confidencial a otros • Tener capacidad suficiente para utilizar la información tecnología de hardware y software • Uso de buenas prácticas para definir contraseñas • Entender y seguir las políticas de seguridad y los	Si Algo No No se sabe			

reglamentos • Reconocer y reportar incidentes				

Hoja de Trabajo. Prácticas de seguridad: Estrategia de Seguridad

Estrategia de Seguridad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Las estrategias comerciales de la organización incorporan consideraciones de seguridad.	Si Algo No No se sabe		.	Rojo Amarillo Verde No aplica
Las estrategias y políticas de seguridad toman en cuenta las estrategias y objetivos del negocio de la organización.	Si Algo No No se sabe			
Las estrategias de seguridad, metas y objetivos son documentados y se revisan de forma rutinaria, se lo actualiza y se comunica a todos los involucrados en la	Si Algo No No se sabe			

organización.				

Hoja de Trabajo. Prácticas de seguridad: Gestión de la Seguridad

Gestión de la Seguridad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
La Gerencia asigna fondos y recursos suficientes para actividades de información de seguridad.	Si Algo No No se sabe			Rojo Amarillo Verde No aplica
Los roles y responsabilidades de seguridad se definen para todo el personal de la organización.	Si Algo No No se sabe			
Todo el personal en todos los niveles de responsabilidad pone en práctica sus funciones asignadas.	Si Algo No No se sabe			
Existen procedimientos documentados para la autorización y				

supervisión de todo el personal (incluido el personal tercerizado) que trabajan con sensible información o que trabajan en lugares donde la información reside.				
Las prácticas de contratación y terminación de personal en la organización se toman en cuenta la seguridad informática.	Si Algo No No se sabe			
La organización gestiona los riesgos de seguridad de la información: • Evalúa los riesgos para la seguridad de la información • Toma medidas para mitigar riesgos de seguridad de la información	Si Algo No No se sabe			

Gerencia recibe y actúa sobre los informes de rutina relacionados con la seguridad de la información (por ejemplo, auditorías, registros y evaluaciones de vulnerabilidad).	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Políticas de Seguridad y Regulaciones

Políticas de Seguridad y Regulaciones				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
La organización cuenta con un amplio conjunto de políticas actuales que periódicamente son revisadas y actualización.	Si Algo No No se sabe			Rojo Amarillo Verde No aplica
Hay un procedimiento documentado de gestión de las políticas de seguridad, que incluye: • Creación • Administración (revisiones periódicas y actualizaciones) • Comunicación	Si Algo No No se sabe			

La organización dispone de un procedimiento documentado para evaluar y garantizar el cumplimiento de las políticas de seguridad, leyes y regulaciones aplicables, y requisitos de seguro.	Si Algo No No se sabe			
La organización uniformemente refuerza sus políticas de seguridad.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Plan de Contingencia/Recuperación de Desastres

Plan de Contingencia/Recuperación de Desastres				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Se ha realizado un análisis de las operaciones, las aplicaciones y los datos críticos.	Si Algo No No se sabe			Rojo Naranja Verde No aplica
La organización ha documentado, revisado y probado: • Planes de continuidad del negocio y de operación en caso de emergencia • Plan de recuperación de desastres (s)	Si Algo No No se sabe			

Los planes de contingencia, recuperación de desastres y de negocios consideran la continuidad física y electrónica y los requisitos de acceso y controles.	Si Algo No No se sabe			
Todo el personal: • Esta consciente de los planes de recuperación de desastres imprevistos y continuidad del negocio. • Comprende y es capaz de realizar sus responsabilidades	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Control de Acceso Físico

Control de Acceso Físico				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Planes de seguridad de las instalaciones y procedimientos para salvaguardar las instalaciones, edificios y cualquier zona restringida y están documentados y probados.	Si Algo No No se sabe			Rojo Naranja Verde No aplica
Hay políticas y procedimientos documentados para la gestión de los visitantes.	Si Algo No No se sabe			

Hay políticas y procedimientos documentados para controlar el acceso físico a las áreas de trabajo y hardware (ordenadores, dispositivos de comunicación, etc.) y soporte de software.	Si Algo No No se sabe			
Las estaciones de trabajo y otros componentes que permiten acceso a la información sensible están físicamente salvaguardados para prevenir el acceso no autorizado.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Gestión del Sistema y la Red

Gestión del Sistema y la Red				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Existen planes de seguridad para salvaguardar el sistema y las redes.	Si Algo No No se sabe			Rojo Naranja Verde No aplica
La información confidencial está protegida en un almacenamiento seguro (por ejemplo, copias de seguridad almacenadas en otro sitio).	Si Algo No No se sabe			
La integridad del software instalado es regularmente verificada.	Si Algo No No se sabe			

Todos los sistemas están actualizados a la fecha de acuerdo con revisiones, parches y recomendaciones de seguridad.	Si Algo No No se sabe			
Existe un plan documentado y comprobado para la copia de seguridad de los datos de software. Todo el personal entiende sus responsabilidades en virtud de los planes de copia de seguridad.	Si Algo No No se sabe			
Todos los cambios de hardware y software son planeados, controlados y documentados.	Si Algo No No se sabe			
Los miembros del área de TI siguen procedimientos para cambiar y dar de baja contraseñas, cuentas y privilegios.	Si Algo No No se sabe			

Solo servicios necesarios están corriendo en los sistemas, todos los servicios que no son necesarios han sido eliminados.	Si Algo No No se sabe			
Herramientas y mecanismos para el sistema de seguridad y administración de la red que se utilizan, se revisan de manera rutinaria, se actualizan o reemplazan.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Monitoreo y Auditoría de la Seguridad de TI

Monitoreo y Auditoría de la Seguridad de TI				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Sistema y red de monitoreo y herramientas de auditoría son habitualmente utilizados por la organización. Actividades extrañas se manejan de acuerdo con las políticas y procedimientos definidos.	Si Algo No No se sabe			Rojo Naranja Verde No aplica
Componentes del Firewall y otros componentes de seguridad son auditados	Si Algo No No se sabe			

periódicamente para revisar el cumplimiento de políticas.				

Hoja de Trabajo. Prácticas de seguridad: Manejo de la Vulnerabilidad

Manejo de la Vulnerabilidad				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Hay un conjunto de procedimientos documentados para manejo de vulnerabilidades, para: • Seleccionar las herramientas de evaluación de vulnerabilidad, listas de control y secuencias de comandos • Mantenerse al día con la vulnerabilidad conocida, tipos y métodos de ataque • Revisar las fuentes	Si Algo No No se sabe			Rojo Naranja Verde No aplica

de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicaciones • Identificación de los componentes de infraestructura a ser evaluado • Programar evaluaciones de vulnerabilidad • interpretar y responder a los resultados • mantener un almacenamiento seguro y la disposición de datos vulnerables				
Se siguen procedimientos de gestión de vulnerabilidades los que son periódicamente revisados y actualizados.	Si Algo No No se sabe			

Evaluaciones de tecnología vulnerable se realizan en forma periódica, y las vulnerabilidades se abordan cuando se las identifica.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Encriptación

Encriptación				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: • Controles apropiados de seguridad se utilizan para proteger información sensible durante el almacenamiento y durante la transmisión (por ejemplo, el cifrado de datos, infraestructura de clave pública, tecnología de red privada virtual).	Si Algo No No se sabe			Rojo Naranja Verde No aplica

Se utilizan protocolos de cifrado cuando se maneja sistemas, routers y firewalls a distancia.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Seguridad de Diseño y Arquitectura

Seguridad de Diseño y Arquitectura				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Arquitectura del sistema y diseño para sistemas nuevos y revisados incluyen las siguientes consideraciones: • Estrategias de seguridad, políticas y procedimientos • Antecedentes de compromisos de seguridad. • Resultados de las evaluaciones de riesgos de seguridad.	Si Algo No No se sabe			Rojo Naranja Verde No aplica

La organización tiene diagramas que muestran la seguridad en toda la empresa y la arquitectura de red que están actualizados.	Si Algo No No se sabe			

Hoja de Trabajo. Prácticas de seguridad: Manejo de Incidentes

Manejo de Incidentes				
Enunciado	**¿Hasta qué punto esta afirmación se refleja en su organización?**	**¿Qué actualmente su organización está haciendo bien en esta área?**	**¿Qué actualmente su organización *no* está haciendo bien en esta área?**	**¿Qué tan efectivamente su organización está implementado las prácticas en esta área?**
Si alguien del personal está encargado de esta área: Existen procedimientos documentados para la identificación, presentación de informes, y procesos para responder a incidentes sospechosos y violaciones.	Si Algo No No se sabe			Rojo Naranja Verde No aplica
Los procedimientos de manejo de incidentes son periódicamente probados, verificados y actualizados.	Si Algo No No se sabe			

Existen políticas y procedimientos documentados para trabajar con autoridades policiales.	Si Algo No No se sabe			

Hoja de Trabajo: Selección de Activos Críticos

Selección de Activos Críticos	
Preguntas a considerar: Qué activo tendría un efecto adverso en la organización si: • ¿Es divulgado a personas no autorizadas? • ¿Es modificado sin autorización? • ¿Se pierde o es destruido? • ¿El acceso al activo es interrumpido?	
Activo Crítico	**Notas**

Hoja de Trabajo: Información de Activos Críticos

Activo Crítico ¿Cuál es el sistema crítico?	**Justificación de la Selección** ¿Por qué es ese sistema crítico para la organización?	**Descripción del Sistema** ¿Quién usa el sistema? ¿Quién es responsable de este sistema?	**Requerimientos de Seguridad** ¿Cuáles son los requerimientos de seguridad para este sistema?	**Requerimiento de seguridad más importante** ¿Cuál de los requerimientos de seguridad es el más importante para este sistema?
			Confidencialidad: Solo personal autorizado puede ver información… **Integridad:** Solo personal autorizado puede modificar información … **Disponibilidad:** … debe estar disponible para que el personal realice su trabajo. **Otro:**	Confidencialidad Integridad Disponibilidad Otro

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red – Perfil básico de riesgo

Actores con acceso a la red – Perfil básico de riesgo

Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*					**Actores de amenazas** *¿Qué actores plantean las mayores amenazas para el sistema a través de la red?*
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	
Red		Adentro	Accidental	Revelación	***Personas que pertenecen a la organización que actúan accidentalmente:***
				Modificación	
				Pérdida	
				Interrupción	
			Premeditado	Revelación	***Personas que pertenecen a la organización que actúan deliberadamente:***
				Modificación	
				Pérdida	
				Interrupción	
		Afuera	Accidental	Revelación	***Personas ajenas a la organización que actúan accidentalmente:***
				Modificación	
				Pérdida	
				Interrupción	
			Premeditado	Revelación	***Personas ajenas a la organización que actúan deliberadamente:***
				Modificación	
				Pérdida	

	Interrupción	

Motivo						**Historia**			
¿Qué tan fuerte es el motivo del actor?			*¿Qué tan confiado está usted de este estimado?*			*¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Alto	**Medio**	**Bajo**	**Muy**	**Algo**	**Nada**		**Muy**	**Algo**	**Nada**
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			
						veces en años			

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red – Áreas de Preocupación

Gente que pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que pertenecen a la organización actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	
De ejemplos de cómo personas que pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	
Gente que no pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que no pertenecen a la organización que actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	
De ejemplos de cómo personas que no pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema

Problemas del Sistema – Perfil básico de riesgo						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Historia** *¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
	Defectos de software	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	El sistema se cae	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	Defectos de hardware	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	Código malicioso	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			

	Interrupción	veces en años			

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Problemas del Sistema – Áreas de Preocupación

Defectos de Software	
De ejemplos de cómo cualquier defecto de software podría ser considerado una amenazar el sistema.	
El sistema se cae	
De ejemplos de cómo si el sistema se cae podría ser considerado una amenazar el sistema.	
Defectos de Hardware	
De ejemplos de cómo cualquier defecto de hardware podría ser considerado una amenazar el sistema.	
Código Malicioso	
De ejemplos de cómo código malicioso de software podría ser considerado una amenazar el sistema.	

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas

Otros Problemas – Perfil básico de riesgo						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Historia** *¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
Portal	Problemas con el suministro de energía	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	Problemas de telecomunicaciones	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	Problemas con sistemas de terceros	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	Desastres naturales	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			

	Interrupción	veces en años			

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas– Áreas de Preocupación

Problemas con el suministro de energía	
De ejemplos de cómo cualquier problema con el suministro de energía podría ser considerado una amenazar el sistema.	
Problemas de telecomunicaciones	
De ejemplos de cómo cualquier problema de telecomunicaciones podría ser considerado una amenazar el sistema.	
Problemas con sistemas de terceros	
De ejemplos de cómo cualquier problema con sistemas de terceros podría ser considerado una amenazar el sistema.	
Desastres naturales	
De ejemplos de algún desastre natural podría ser considerado una amenazar el sistema.	*No se han registrado amenazas al sistema por desastres naturales.*

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas

Otros Problemas – Perfil básico de riesgo						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Historia** *¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?*	*¿Qué tan exactos son estos datos?*		
Activo	**Actor**	**Resultado**		**Muy**	**Algo**	**Nada**
	Personas clave permiso temporal	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			
	` Personas clave que renuncian	Revelación	veces en años			
		Modificación	veces en años			
		Pérdida	veces en años			
		Interrupción	veces en años			

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas– Áreas de Preocupación

Personas clave que toman un permiso temporal	
De ejemplos de cómo si una persona clave en la organización toma un permiso temporal podría ser considerado una amenazar el sistema.	
Personas clave que salen de la organización permanentemente	
De ejemplos de cómo si una persona clave en la organización se retira de la empresa permanentemente podría ser considerado una amenazar el sistema.	

Hoja de Trabajo: Rutas de acceso

Sistema de interés	
Puntos de Acceso	
Sistema de Interés	**Puntos de Acceso Intermedios**
Sistema de Interés *¿Cuál de las siguientes clases de componentes son parte del sistema de interés?*	**Puntos de Acceso Intermedios** *¿Cuál de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones desde el sistema de interés hacia la gente?* *¿Cuál de las siguientes clases de componentes podría servir como un punto de acceso intermedio?*
Servidores Redes Internas Estaciones de trabajo Otros	Red Interna Red externa Otros

Puntos de Acceso		
Acceso al Sistema por Individuos	**Ubicación de donde se almacenan los datos**	**Otros Sistemas o Componentes**
Acceso al Sistema por Individuos *¿De cuál de las siguientes clases de componentes puede la gente (por ejemplo, los usuarios, los atacantes) acceder al sistema de interés?* *Considere puntos de acceso internos y externos a la red de la organización*	**Ubicación de donde se almacenan los datos** *¿En qué clase de componente esta la información del sistema de interés almacenada por motivos de respaldo?*	**Otros Sistemas o Componentes** *¿Cuál otro sistema accede a información del sistema de interés?*
Estaciones de Trabajo Laptops PDAs/Componentes Wireless Estaciones de Trabajo fuera de la oficina Otros	Dispositivos de almacenamiento de respaldos locales Otros	

Hoja de Trabajo: Evaluación de la infraestructura

Clase *¿Cuál clase de componente está relacionado con uno o más de los activos críticos?*	**Activo Crítico** *¿Cuál activo critico está relacionado con cada clase?*			**Responsabilidad** *¿Quién es responsable de mantener y asegurar cada clase de cada componente?*
	Portal	**Aplicaciones**	**Cliente**	
Servidores				
Red interna				
Estaciones de trabajo				
Laptops				
PDAs/Componentes Wireless				

Dispositivos de Almacenamiento				
Red Externa				
Estaciones de trabajo fuera de la oficina				

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red. Impacto

Actores con acceso a la red – Impacto												
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*						**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**		**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
Red		Adentro	Accidental	Revelación							
				Modificación							
				Pérdida							
				Interrupción							
			Premeditado	Revelación							
				Modificación							
				Pérdida							
				Interrupción							
		Afuera	Accidental	Revelación							
				Modificación							
				Pérdida							
				Interrupción							
				Revelación							

	Premeditado	Modificación						
		Pérdida						
		Interrupción						

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema. Impacto

Problemas del Sistema – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
	Defectos de software	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
	El sistema se cae	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
	Defectos de hardware	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
		Revelación						

	Código malicioso	Modificación						
		Pérdida						
		Interrupción						

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Impacto

Otros Problemas – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
	Problemas con el suministro de energía	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
	Problemas de telecomunicaciones	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
	Problemas con sistemas de terceros	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
		Revelación						

	Desastres naturales	Modificación						
		Pérdida						
		Interrupción						

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Impacto

Otros Problemas – Impacto								
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Impacto** *¿Cuál es el impacto potencial en la organización en cada área aplicable?* *A: Alto* *M: Medio* *B: Bajo*					
Activo	**Actor**	**Resultado**	**Reputación**	**Financiero**	**Productividad**	**Multas**	**Seguridad**	**Otro**
	Personas clave permiso temp.	Revelación						
		Modificación						
		Pérdida						
		Interrupción						
`	Personas clave que renuncian	Revelación						
		Modificación						
		Pérdida						
		Interrupción						

Hoja de Trabajo: Criterios basados en la frecuencia

	1. Piense en lo que constituye un riesgo alto, medio y bajo de la ocurrencia de amenazas a los activos críticos de la organización.				
	Alto				**Medio**
Tiempo entre eventos	*Diario*	*Semanal*	*Mensual*	*Cuatro veces al año*	*< 4 veces al año*
Frecuencia analizada					

	2. Dibuje líneas que separen alto de medio y medio de bajo				
Medio	**Bajo**				
Una vez al año	*< 1 vez al año*	*Una vez cada 5 años*	*Una vez cada 10 años*	*Una vez cada 20 años*	*Una vez cada 50 años*

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia - Actores con acceso a la red. Probabilidad

Actores con acceso a la red – Probabilidad

Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*					**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo) ¿Qué tan confiado está de esta estimación?*			
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Valor**	**Confianza**		
						Muy	**Algo**	**Nada**
Red	Red	Adentro	Accidental	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
			Premeditado	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
		Afuera	Accidental	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
			Premeditado	Revelación				
				Modificación				
				Pérdida				

	Interrupción				

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Problemas del Sistema. Probabilidad

Problemas del Sistema – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
	Defectos de software	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	El sistema se cae	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	Defectos de hardware	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	Código malicioso	Revelación				
		Modificación				

	Pérdida				
	Interrupción				

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Probabilidad

Otros Problemas – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
	Problemas con el suministro de energía	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	Problemas de telecomunicaciones	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	Problemas con sistemas de terceros	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
	Desastres naturales	Revelación				
		Modificación				
		Pérdida				

	Interrupción				

Hoja de Trabajo: Perfil de riesgo para el activo crítico Portal de Gerencia – Otros Problemas. Probabilidad

Otros Problemas – Probabilidad						
Amenaza *¿Para cuál rama hay una posibilidad no desdeñable de una amenaza al activo? Marque estas ramas en el árbol.* *¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.*			**Probabilidad** *¿Qué tan probable es que la amenaza ocurra en el futuro? (A: Alto, M: Medio, B: Bajo)* *¿Qué tan confiado está de esta estimación?*			
Activo	**Actor**	**Resultado**	**Valor**	**Confianza**		
				Muy	**Algo**	**Nada**
	Personas clave permiso temp.	Revelación				
		Modificación				
		Pérdida				
		Interrupción				
`	Personas clave que renuncian	Revelación				
		Modificación				
		Pérdida				
		Interrupción				

Hoja de Trabajo: Conocimiento de seguridad y entrenamiento

¿Qué tan formal es la estrategia de capacitación de su organización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Estrategia de Protección		
La organización cuenta con una estrategia de capacitación documentada que incluye una evaluación del conocimiento de seguridad para la sensibilización y la formación en materia de seguridad para las tecnologías de apoyo.	Actual	Cambiar
La organización tiene una estrategia de capacitación informal e indocumentada.	Actual	Cambiar

¿Qué tan seguido se realizan entrenamientos de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Evaluar el conocimiento de Seguridad		
Se proveen entrenamientos periódicos sobre seguridad que a todos los empleados 1 vez cada año.	Actual	Cambiar
Se provee entrenamiento sobre seguridad a personas nuevas en la organización como parte de sus actividades de orientación.	Actual	Cambiar
La organización no provee un entrenamiento sobre seguridad. Cada miembro del personal aprende sobre problemas de seguridad por sí mismo.	Actual	Cambiar

¿En qué medida se requiere que los miembros del área de TI asistan a un entrenamiento relacionado con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento relacionado con Seguridad		
Los miembros del área de TI deben asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	Actual	Cambiar
Los miembros del área de TI pueden asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen si ellos lo piden.	Actual	Cambiar
La organización no provee oportunidades para que miembros del área de TI asistan a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	Actual	Cambiar

¿Qué tan formal es el mecanismo de su organización para proveer actualizaciones periódicas de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Actualizaciones periódicas de Seguridad		
La organización tiene mecanismos formales para proveer miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	Actual	Cambiar
La organización no tiene un mecanismo para proveer a miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	Actual	Cambiar

¿Cuál es el mecanismo oficial de su organización para verificar que el personal reciba capacitación? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Verificación del Entrenamiento		
La organización tiene mecanismos formales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual	Cambiar
La organización tiene mecanismos informales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual	Cambiar
La organización no tiene mecanismos para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual	Cambiar

Hoja de Trabajo: Estrategia de protección para el manejo colaborativo de la seguridad

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con colaboradores y socios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Colaboradores y Socios		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con colaboradores y socios.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con colaboradores y socios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con colaboradores y socios.	Actual	Cambiar
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con colaboradores y socios.	Actual	Cambiar

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con contratistas y subcontratistas? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Contratistas y Subcontratistas		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con contratistas y subcontratistas. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con contratistas y subcontratistas.	Actual	Cambiar
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	Actual	Cambiar

¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con proveedores de servicios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Proveedores de Servicios		
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con proveedores de servicios.	Actual	Cambiar
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con proveedores de servicios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con proveedores de servicios.	Actual	Cambiar
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con proveedores de servicios.	Actual	Cambiar

¿Hasta qué punto la organización comunica formalmente sus requisitos de protección de la información a terceras partes? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Requerimientos		
La organización documenta los requisitos de protección de la información y las comunica explícitamente a terceras partes.	Actual	Cambiar
La organización comunica informalmente los requisitos de protección de información a terceras partes.	Actual	Cambiar
La organización no comunica sus requisitos de protección de información a terceras partes.	Actual	Cambiar

¿Hasta qué punto la organización verifica que terceras partes estén cumpliendo con los requisitos de protección de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Verificación		
La organización tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual	Cambiar
La organización tiene mecanismos informales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual	Cambiar
La organización no tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual	Cambiar

¿Hasta qué punto el programa de entrenamiento sobre conocimiento de seguridad de su organización incluye manejo colaborativo de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Conocimiento del Personal		
El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año.	Actual	Cambiar
El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a los nuevos empleados como parte de sus actividades de orientación.	Actual	Cambiar
El programa de entrenamiento sobre conocimiento de seguridad de la organización no incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año. Los miembros del personal aprenden sobre manejo colaborativo de la seguridad por si mismos.	Actual	Cambiar

Hoja de Trabajo: Estrategia de protección para monitorear y auditar seguridad física

¿Quién es actualmente responsable para monitorear y auditar la seguridad física? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Responsabilidad						
Tarea:	Actual			Cambiar		
	Interno	Externo	Combinado	Interno	Externo	Combinado
Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware.						
Monitorear acceso físico controlado por hardware.						
Monitorear acceso físico controlado por software.						
Monitorear acceso físico a áreas de trabajo restringidas.						
Revisar los registros de monitoreo periódicamente.						
Investigar y monitorear cualquier actividad inusual no identificada.						

¿Hasta qué punto son los procedimientos de esta área formalmente documentados? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Procedimientos		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización ha documentado formalmente planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual	Cambiar
La organización ha documentado formalmente algunos planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software. Algunas políticas y procedimientos son informales y no son documentados.	Actual	Cambiar
La organización tiene planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software que son informales y no documentados.	Actual	Cambiar

¿Hasta qué punto se requiere que el personal de su organización asista a entrenamientos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
Miembros designados del personal están obligados a asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual	Cambiar
Miembros designados del personal pueden asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software si ellos lo piden.	Actual	Cambiar
La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual	Cambiar

Hoja de Trabajo: Estrategia de protección para autenticación y autorización

¿Quién es actualmente responsable de la autenticación y autorización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Responsabilidad						
Tarea:	Actual			Cambiar		
	Interno	Externo	Combinado	Interno	Externo	Combinado
Implementar control de acceso (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.						
Implementar autenticación de usuarios (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.						
Establecer y terminar acceso a sistemas e información para ambos individuos y grupos.						

¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Procedimientos		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización ha documentado formalmente autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar
La organización ha documentado formalmente autorización y autenticación de algunos procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red. Algunos procedimientos en esta área son informales y no están documentados.	Actual	Cambiar
La organización tiene procedimientos informales y no documentados para la autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar

¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Entrenamiento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
Miembros designados del personal están obligados a asistir a entrenamientos para implementar medidas tecnológicas para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar
Miembros designados del personal pueden asistir a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red si ellos lo piden.	Actual	Cambiar
La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual	Cambiar

Hoja de Trabajo: Estrategia de protección para políticas de seguridad y regulaciones

¿Hasta qué punto están formalmente documentadas las estrategias de protección relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Políticas Documentadas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene un conjunto integral de políticas relacionadas con seguridad formalmente documentadas.	Actual	Cambiar
La organización tiene un conjunto integral de políticas relacionadas con seguridad informalmente documentadas.	Actual	Cambiar
Las políticas relacionadas con seguridad de la organización son informales y no están documentadas.	Actual	Cambiar

¿Qué tan formal es el mecanismo de su organización para crear y actualizar sus políticas relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Manejo de Políticas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene un mecanismo formal para crear y actualizar su política relacionada con seguridad.	Actual	Cambiar
La organización tiene un mecanismo formal para crear su política relacionada con seguridad. La organización tiene un mecanismo informal y no documentado para actualizar su política relacionada con seguridad.	Actual	Cambiar
La organización tiene un mecanismo informal y no documentado para crear y actualizar su política relacionada con seguridad.	Actual	Cambiar

¿Qué tan formal son los procedimientos de su organización para aplicar sus políticas relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Aplicación de Políticas		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene procedimientos formales para aplicar su política relacionada con seguridad. Estos procedimientos aplicados son aplicados y seguidos constantemente.	Actual	Cambiar
La organización tiene procedimientos formales para aplicar su política relacionada con seguridad. Estos procedimientos aplicados nunca se siguen.	Actual	Cambiar
La organización tiene un mecanismo informal y no documentado para aplicar su política relacionada con seguridad.	Actual	Cambiar

¿Qué tan formales son los procedimientos de su organización para cumplir con las políticas y regulaciones relacionadas con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?

Políticas y Cumplimiento del Reglamento		
Si el personal de su organización es parcial o completamente responsable por esta área:		
La organización tiene procedimientos formales para cumplir con políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro.	Actual	Cambiar
La organización tiene procedimientos formales para cumplir con ciertas políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro. Algunos procedimientos en esta área son informales y no están documentados.	Actual	Cambiar
La organización tiene procedimientos informales y no documentados para cumplir con políticas de seguridad de la información, leyes aplicables, regulaciones y requisitos del seguro.	Actual	Cambiar

Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Conocimiento de seguridad y entrenamiento*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*

Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Manejo colaborativo de la seguridad*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*

Hoja de Trabajo: Plan de Mitigación

Área de Mitigación: *Monitorear y auditar seguridad física*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*

Hoja de Trabajo: Autenticación y autorización

Área de Mitigación: *Autenticación y autorización*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*

Hoja de Trabajo: Políticas de seguridad y regulaciones

Área de Mitigación: *Políticas de seguridad y regulaciones*

Actividad de mitigación *¿Qué actividad de mitigación va a implementar en esta área de seguridad?*	**Razón** *¿Por qué seleccionó esta actividad?*

Responsable de mitigación *¿Quién necesita estar involucrado en implementar cada actividad?*	**Apoyo adicional** *¿Qué apoyo adicional se necesitará cuando se implemente cada actividad?*

Hoja de Trabajo: Identificar siguientes pasos

Considere:

- *Contribuir fondos para las actividades de seguridad de la información.*
- *Asignar personal para las actividades de seguridad de la información.*
- *Asegurarse que los funcionarios dispongan de tiempo suficiente asignado a las actividades de seguridad de la información.*
- *Permitir al personal recibir entrenamiento sobre seguridad de la información.*
- *Hacer que la seguridad de la información sea una prioridad estratégica.*

Gestión para la mejora de la Seguridad	**Monitorear la implementación**	**Ampliar la actual evaluación de riesgos en la seguridad de la información**	**Siguiente evaluación de riesgos en la seguridad de la información**
¿Qué debe hacer la Gerencia para apoyar la implementación de los resultados de Octave-S?	*¿Qué debe hacer la información para rastrear el progreso y asegurar que los resultados de esta evaluación se implementen?*	*¿Expendería la actual evaluación OCTAVE-S para incluir activos críticos adicionales? ¿Cuáles?*	*¿Cuándo conducirá la organización su siguiente evaluación OCTAVE-S?*

ANEXO C: INFORME DE RETROALIMENTACIÓN DE PIRÁMIDE DIGITAL

www.piramidedigital.com
El mayor Portal de Gerencia en Español

Quito, septiembre de 2013

Señorita
OLGA PÁEZ
Estudiante de la
Facultad de Ingeniería de la
Pontificia Universidad Católica del Ecuador
Presente

De mis consideraciones

Por medio del presente, en mi calidad de Gerente General y Representante Legal de **PIRAMIDE DIGITAL CIA. LTDA.** certifico que la señorita **OLGA PÁEZ** realizó la evaluación de riesgos y seguridad utilizando la metodología de Octave – S, para el efecto ella contó con personal la ayuda y soporte que pudo brindar personal de mi organización, ofreciéndole toda la información que requería para la realización del trabajo antes indicado.

Después de realizar la evaluación conjunta entre Pirámide Digital y la Srta. Páez, concluimos:

- Contar con un programa de entrenamiento sobre conocimiento de seguridad para todo el personal.
- Definir políticas para determinar roles y responsabilidades del personal.
- Documentar planes y procedimientos para monitoreo del acceso físico y autenticación de usuarios.
- Asegurarse que el personal conozca los procedimientos de seguridad.
- Después de terminar con la evaluación, se concluye que la metodología que propone Octave es la mejor entre las opciones existentes ya que es flexible, cubre muchos ámbitos y permite trabajar directamente con el personal de la organización para asegurarse que los datos recolectados sean lo más acertados.
- Hubo un excelente proceso de aprendizaje para todo el personal involucrado.

Pirámide Digital agradece la participación de la Srta. Páez en el proceso de implementación de la norma Octave-S; ha sido un reto profesional de mucha importancia que nos ha permitido crecer como organización y ha sido un aporte significativo por parte de la Srta. Páez a quien agradecemos y deseamos éxitos en su vida profesional

Atentamente,

PABLO G. PAEZ, PhD
Gerente General
PIRAMIDE DIGITAL CIA. LTDA.
Av. 12 de Octubre y Cordero, Edificio World Trade Center Torre B, Oficina 702
Quito - Ecuador
Teléfonos: 2556622, 2556623, 2909455
Celular: 091699699
Mail: pablo_paez@piramidedigital.com

Oficina Matriz: Av. 12 de Octubre y Cordero. Ed World Trade Center, Torre B, Oficina 702 Tel. +(593)2 255 66 22, 255 66 23 Fax +(593)2 255 98 88 Cel (593)91 699699 Quito – Ecuador Skype:PiramideDigital

Centro de Capacitación Gerencial. Juan Pascoe y Myriam de Sevilla. Campos Verdes. Sector Cuendina. Pichincha, Ecuador. Tel/Fax +(593-2) 2339744, 2080300 Cel (593)99 922000 Sangolquí – Ecuador Skype:pdccgec