DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ANGELCOM S.A.

DIANA CAROLINA HERNÁNDEZ MEDINA

CÓDIGO: 062041534

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERÍA

INGENIERÍA INDUSTRIAL

BOGOTÁ D.C

2011

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ANGELCOM S.A.

PROYECTO DE GRADO PRESENTADO COMO PRERREQUISITO PARA OBTENER EL TÍTULO DE INGENIERO INDUSTRIAL

DIANA CAROLINA HERNÁNDEZ MEDINA

CÓDIGO: 062041534

DIRECTOR

Ing. SONIA LUCIA MENESES VELOSA

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERÍA

INGENIERÍA INDUSTRIAL

BOGOTÁ D.C

2011

Nota de aceptaciòn

_____

_____

_____

_____

_____

Jurado

_____

Jurado

Bogotá D.C. Febrero 2011

AGRADECIMIENTOS

En primer lugar, quiero dar gracias por su afecto y amistad a todos los compañeros, amigos y conocidos con los que he compartido el viaje, de años de esfuerzo y dedicación en la Universidad Libre.

De la misma manera, quiero reconocer a todos mis profesores y directivos la labor, en ocasiones no demasiado fácil, de transmitir sus conocimientos que suponen y supondrán la inspiración necesaria para los futuros grandes retos que llegue a plantear la vida.

Por último, pero no menos importante, agradecer a mi madre y hermanas el apoyo y confianza depositada en mí en todo momento para culminar una de tantas metas y proyectos de vida.

Gracias a todos.

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICOS

TABLA DE FIGURAS

LISTA DE SIGLAS

SGSI: Sistema de Gestión de Seguridad de la Información.

BIA: Business Impact Analysis

BCP: Plan de Continuidad del negocio

PTR: Plataforma tecnológica de recaudo

SGC: Sistema de Gestión de Calidad

UKAS: The United Kingdom Acreditation Service-

BSI: British Standard Institute

COSO:The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework,

LEY SOX: La Ley Sarbanes-Oxley (SOX), de EE.UU

ITIL: Information Technology Infrastructure Library",

COBIT: Control Objectives for Information and related Technology"

AS: Aseguramiento del Servicio

CIG: Centro de Información y Gestión

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ANGELCOM S.A.

RESUMEN

El presente proyecto es el resultado de la realización del análisis de la empresa Angelcom S:A, ubicada en la ciudad de Bogotá, para evaluar el nivel de seguridad de la información y sus procesos estratégicos.

Primeramente, se estudio la organización desde una óptica del Sistema de Gestión de Calidad para evaluar cuál es su situación respecto a estos términos, para así comenzar a enumerar los riesgos que la afectarían, así como el impacto que producirían éstas en la organización en el caso de que llegara a producirse una amenaza.

De esta manera se determinaron cuáles son las vulnerabilidades, y qué medidas sería necesario adoptar para conseguir dotar a la misma de un nivel de seguridad adecuado para proteger su información en función de los requerimientos contractuales del cliente Transmilenio S.A

Como resultado del Diseño del Sistema de Gestión de Seguridad de Información se encontró que los procesos a nivel organizacional tales como Aseguramiento del Servicio y Centro de Información y Gestión, en cuestiones de Confidencialidad, integridad y disponibilidad son los más críticos; que cuantitativamente hablando generarían impactos tanto financieros como operacionales demasiado altos, y a nivel contractual la organización se vería afectado para próximas renovaciones y/o asignaciones de licitaciones contractuales.

Durante el análisis según el diseño metodológico propuesto, se logró identificar los activos de información de cada uno de los procesos en mención, bajo las posibles amenazas y vulnerabilidades a los cuales estaban expuestos; adicionalmente se pudo verificar los riesgos de información para cada proceso, teniendo en cuenta el impacto de la amenaza, su probabilidad de ocurrencia y su priorización. Estos riesgos se han caracterizado en un mapa de riesgos los cuales han sido evaluados y permite evidenciar lo siguiente:

- Tipo de riesgo
- Probabilidad
- Impacto
- Tipo de Control
- Criterio de Valoración de control
- Criterio de aceptación del riesgo

Con lo anterior, permitió dar un tratamiento a los riesgos de información adecuados y asociados a los procesos en mención.

Finalmente, con la información recopilada en el presente estudio, la organización pudo haber tomado las acciones necesarias para mejorar la seguridad de la información ya que a nivel organizacional se encuentra altamente expuesta a pérdidas, fraude y robos de información. Sin embargo la organización o principalmente la Alta Dirección considera que cubre todas las actividades de control relacionados con los procesos para satisfacer los requisitos del cliente en cuanto a seguridad de la información.

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

1.1.1 ANTECEDENTES

La “Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua con ella.”

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). Los descubrimientos arqueológicos marca, sin duda, las más importantes pruebas de seguridad de los antiguos: Las pirámides egipcias, el palacio de Sargon, el templo Karnak en el Valle de Nilo entre otros.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos que los animales: luchando o huyendo para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alamar y reaccionar ya eran manejados por ellos.

Como todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias y esto se convirtió en un elemento limitante; el cual se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de República Romana. El próximo paso de la seguridad fue la especialización. Así nace la seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la seguridad

Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma).

Desde el siglo XVII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad.

La seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente un teórico y pionero del Management, Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir un objetivo de seguridad se puede denotar lo siguiente:"salvalguar propiedades y personas contra el robo, fuego, inundaciones, contrarrestar huelgas, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Las medidas de seguridad a las que se refiere Fayol, solo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente: los equipos, ni siquiera el empleado.

Hoy día la seguridad tiene dos puntos de vista, el legislativo y el técnico. El legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio desde el punto de vista técnico la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y

el conocimiento en este nuevo milenio. Desde este punto de vista el objeto del presente proyecto tendrá gran relevancia ya que permitirá dar un lineamiento más específico para la continuidad del negocio.

En los inicios de la década de los noventa del siglo pasado, se inició el desarrollo de un modelo "Sistema de Gestión de Seguridad de Información" en Inglaterra. El Brithish Stadars Institute fue el promotor. En 2005, la organización internacional para la normalización, hizo, oficializo la norma, denominándola "Sistema de Gestión de Seguridad de Información" ISO 27001:2005. Esa es la que los mercados internacionales empiezan exigir a las empresas, para poder demostrar que la información que manejan está bajo las características de confidencialidad, integridad y disponibilidad, y que garantizan continuidad en las operaciones, por que cuenta con un sistema para la planificación de la continuidad del negocio. Una empresa con la norma implantada garantiza en la cadena de suministros que es proveedor confiable.

La formalización de estándares de seguridad informática en el país, es un factor decisivo para movilizar los intereses de las empresas, gobierno e industria, hacia una cultura de seguridad informática más profesional e internacional, que responda a los exigentes entornos competitivos actuales. [1]Por esta razón podemos tomar como ejemplo y nombrar a la organización UNE que es la primera en Colombia en certificarse en Sistema de Gestión de Seguridad de la Información, con esta certificación, los clientes UNE cuentan con el respaldo, los más altos niveles de calidad y gestión en la protección de su información. La certificación ISO/IEC 27001:2005 fue recomendada por Bureau Veritas Certification ante los servicios de acreditación del Reino Unido- UKAS.
Tras un período de evaluación y aprobación de los procesos, la firma Bureau Veritas certificó el Sistema de Gestión de Seguridad de la Información de UNE EPM Telecomunicaciones basado en la norma ISO/IEC 27001:2005. UNE es la primera

[1] Boletín UNE No. 162 - UNE certifica Sistema de Gestión de la Seguridad de la Información (Bogotá, octubre 19 de 2009)

compañía de telecomunicaciones en el país en obtener un certificado de esta magnitud. La obtención de certificados reconocidos internacionalmente a través de entes como Bureau Veritas Certification y The United Kingdom Acreditation Service-UKAS, para una empresa como UNE, confirma a sus clientes el mejoramiento continuo de la compañía, a través de la gestión sincronizada de la infraestructura tecnológica, los procesos y el capital humano. Según la firma Bureau Veritas Certification, "UNE EPM Telecomunicaciones, patrimonio de los colombianos, es una empresa joven que desde su nacimiento ha preparado tanto su personal como su tecnología para brindar en todo momento el mejor de los servicios, buscando las relaciones más duraderas con sus clientes y mostrándose a la vanguardia con respecto a las demás compañías del sector, pues se convierte en la primera compañía en certificar su Sistema de Gestión de la Seguridad de la Información".

La certificación ISO/IEC 27001:2005 se suma a las certificaciones de los Sistemas de Gestión de Calidad en las Normas ISO 9001:2008 y NTC GP1000:2004, lo cual se traduce en un avance significativo de la Compañía en el sector de las telecomunicaciones en Colombia y en el mundo; la capacidad de mejorar cada día más su desempeño; y entregar productos y servicios que respondan a las necesidades y expectativas de los clientes.

Para el presidente de UNE, Horacio Vélez de Bedout, "este hecho permitió que todos nuestros clientes cuenten con la gestión en protección de su información y con la confianza de que nuestra empresa ha adoptado las medidas para tratar los riesgos asociados a su disponibilidad, confidencialidad e integridad". Bureau Veritas Certification tiene una lista de más de 100 mil empresas certificadas en más de 140 países en el mundo, más de 10 mil en Latinoamérica y alrededor de 2.200 de ellas en Colombia. Con este nuevo logro, UNE continúa avanzando en prestar el mejor servicio a sus clientes, optimizar sus procesos y lograr ser la empresa integrada de telecomunicaciones más competitiva de Colombia.

Debido al gran valor de la información y al gran impacto que tiene sobre las organizaciones el riesgo en su integridad, la ISO ha desarrollado un conjunto de normas que ayuda a las empresas a gestionar sus activos de información, con el fin de garantizar la continuidad del negocio y la eficiencia de sus procesos.

Hoy en día las empresas deben enfocar parte de su atención en el grado de la vulnerabilidad y en las herramientas de seguridad con las que cuentan, para hacerle frente a posibles amenazas informáticas, ya que se pueden traducir en pérdidas cuantiosas de dinero o en su defecto en multas por incumplimiento a requerimientos contractuales. Para protegerse ante ciertas amenazas, no basta que las empresas posean dispositivos de protección informática; sino que el funcionamiento de los mismos ha de estar marcado por la implicación de todas las áreas de la organización y por ende de todo el personal involucrado. También es cierto que no solo se trata de tecnología sino de tener en cuenta siempre las tres variables que marcan la diferencia para la disminución del riesgo: Tecnología, proceso y personas; que en cada uno de estos puntos hay mucho por hacer, es decir; considerando los niveles de confidencialidad, disponibilidad e integridad que requiere cada uno de los elementos ponderados de las funciones del manejo de la seguridad informática y del negocio.

Las empresas están empujando el desarrollo de la seguridad informática en Colombia, frente a una gran empresa que fortalece sus esquemas vigentes; mostrando un ligero cambio en la creación de áreas de seguridad informática en el país.

Es necesario adelantar estudios y prácticas comparativas de los costos que se derivan de los incidentes de seguridad informática para construir una base sistemática de análisis que permita a las organizaciones, estimar y proponer modelos de inversión en seguridad informática acordes con su realidad de negocios y el escenario cambiante de la seguridad informática.

La formalización de estándares de seguridad informática en el país, es un factor decisivo para movilizar los intereses de las empresas, gobierno e industria, hacia una cultura de seguridad informática más profesional e internacional, que responda a los exigentes entornos competitivos actuales.

De los comienzos de la Gestión de seguridad de la información hasta la ISO 27001:2005 se toma como base los siguientes antecedentes:

- A principios de 1990- Departamento de Comercio e Industria del Reino Unido apoyó su desarrollo.
- 1995-Por primera vez se adopta como norma inglesa BSI
- 1998-Se lanzan los requisitos para su certificación.
- 1999-Se emite una segunda edición de la norma
- 2000-Fue aprobada como la parte 1 de ISO 17799
- 2002-BS 7799-2 se publico el 5 de septiembre: en esta revisión se adoptó el “modelo de proceso” con el fin de alinearla con ISO 9001 en ISO 14001.
- Hasta 2003, habían sido emitidos cerca de 500 certificados.
- A finales del 2004, cerca de 950 compañías se habían certificado en BS 7799-2.
- 15 de Octubre de 2005-Se aprueba la Norma ISO 27001-2005 y en 2006 existen ya más de 2030 compañías certificadas a nivel mundial.

ESTÁNDARES Y BUENAS PRÁCTICAS EN SEGURIDAD INFORMÁTICA Y REGULACIONES EN SEGURIDAD DE LA INFORMACIÓN

Esta pregunta muestra que en Colombia, ISO/IEC 27001, Cobit, Nist, e ITIL son las prácticas más utilizadas en el área de seguridad de la información dentro de las organizaciones.

Su utilización implica crear procesos metódicos de trabajo para construir modelos adecuados de protección de la información en las organizaciones.

PRICE WATERHOUSECOOPERS (COLOMBIA-2009) GLOBAL STATE OF INFORMATION SECURITY STUDY

Estándar o Buena Práctica	2008 %	2009 %
ISO 27001	45,80	49,0
Common Criteria	5,20	2,6
Cobit 4.1	23,40	21,6
Magerit	5,20	5,2
Octave	2,3	3,1
Guías NIST	12,30	14,4
Guías ENISA	2,3	0,5
Top SANS	7,10	5,2
OSSTM	7,50	5,2
ISM3	3,90	2,6
ITIL	26.90	35,1
Servicios de Auditoría Especializada	-	12,9
No se consideran	37,70	22,2
Otra	10,20	7,7

TABLA 1.

CERTIFICACIONES EN SEGURIDAD INFORMÁTICA A NIVEL NACIONAL

PRICE WATERHOUSECOOPERS (COLOMBIA-2009) GLOBAL STATE OF INFORMATION SECURITY STUDY

	2007 %	2008 %	2009%
Ninguna	60,3	57,90	46,4
CISSP	20,7	20,50	15,5
CISA	14,9	13,80	10,8
CISM	9,9	11,80	13,4
CFE	0,8	4,0	3,6
CIFI	5,8	4,0	4,1
CIA	10,7	8,40	6,7
GIAC SANS	-	-	3,6
Security+	-	5,91	6,2
NSA IAM/IEM	-	-	1,0
Otras: Especializaciones en Auditoría de Sistemas, Especializaciones en Seguridad Informática, Diplomados en Seguridad Informática, Auditor Líder BS7799, Certified Ethical Hacking, CCNA, CCSP, GSEC, MCSE, etc.	18,2	13,8	11,9

TABLA 2.

En Colombia vemos una disminución moderada en el personal que dice no contar con certificaciones de seguridad de la información. Un aumento moderado se refleja en la certificación CISM, certificaciones orientadas a los temas de gerencia de la seguridad de la información. Se mantiene un interés por la certificación CISSP.

Estos resultados reiteran el llamado a la academia para atender la demanda de formación en estas áreas, nuevo perfil exigido por las organizaciones para fortalecer los esquemas de seguridad y control, de cara a la exigencia de un escenario globalizado. Dentro del grupo de las otras certificaciones, es importante resaltar que algunos encuestados hablaron de CEH, como una certificación importante, a la hora de trabajos con la seguridad de la información.

En tal sentido, lo que se está buscando son especialistas certificados en *ethical hacking*, una tendencia local en aumento, que requiere especialistas formados en la materia.

La inversión en seguridad de la información se encuentra concentrada todavía en tecnología como las redes y sus componentes, además de la protección de datos de los clientes y un ligero interés en el tema de control de la propiedad intelectual y derechos de autor. Son motivadores de la inversión en seguridad: la continuidad de negocio, el cumplimiento de regulaciones y las normativas internas y externas, así como la protección de la reputación de la empresa. Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de la seguridad de la información.

Actualmente, la norma de la super-financiera comienza a cambiar el panorama de la seguridad de la información en la Banca y en el país. La industria en Colombia exige más de dos años de experiencia en seguridad informática, como requisito para optar por una posición en esta área. De igual forma, se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero aún la oferta de programas académicos formales se encuentra limitada, lo que hace que las organizaciones opten por contratar a profesionales con poca experiencia en seguridad y decidan formarlos localmente. Las certificaciones CISSP, CISA y CISM son las más valoradas por el mercado y las que a la hora de considerar un proyecto de seguridad de la información, marcan la diferencia para su desarrollo y contratación.

Las cifras en 2009 muestran los mecanismos tradicionales de protección entre ellos los antivirus, las contraseñas, los firewalls de software y hardware, como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies, así como un aumento creciente por el uso de certificados digitales. Existe un marcado interés por las herramientas de cifrado de datos y los firewalls de aplicaciones web, que establecen dos tendencias emergentes, ante las frecuentes

fugas de información y migración de las aplicaciones web, al contexto de servicios o web services.

De igual manera que las tendencias mundiales, los virus son considerados como una de las fuentes mejor identificadas, frente a los incidentes de seguridad, tratados en la actualidad en forma más continua, pero con pocos procedimientos formales para su manejo. Aunque existe una legislación en temas de delito informático en el país, llevar a cabo un proceso jurídico puede resultar costoso

Los sistemas de gestión de seguridad de la información demandan en las organizaciones mayores esfuerzos, que parten desde las políticas de seguridad de la información, uno de los talones de Aquiles en los procesos de ese entorno. Los estándares internacionales de la industria se ven reflejados en Colombia en las buenas prácticas en seguridad de la información. De ahí que el ISO 27000, el Cobit 4.1 y las Guías del NIST sean bien aceptados en los departamentos de tecnología informática.

1.1.2 FORMULACIÓN DEL PROBLEMA

El presente estudio pretende la transformación de la seguridad de la información de Angelcom S. A., con el fin de aumentar su competitividad dentro de un lineamiento de proveedor confiable para operar como concesión en la explotación económica del Recaudo del Sistema TransMilenio S.A.

Toda la información que se produzca como resultado de dicha explotación de la concesión del recaudo es de propiedad de TransMilenio S.A., por lo tanto, la organización deberá garantizar la no utilización y divulgación de información para fines diferentes a la gestión del recaudo. La complejidad del manejo de la seguridad de la información hace que sea necesario desarrollar un diseño de un Sistema de Gestión de Seguridad de la información que sirva para administrar la información, y se asocie con la protección de los activos informáticos.

La adopción de un SGSI estuvo influenciado por las necesidades propias de la organización, los requisitos de seguridad, (análisis y evolución de riesgos) los procesos empleados y la estructura de la misma; para que a mediano plazo se piense en una posible certificación.

1.1.3 DESCRIPCIÓN DEL PROBLEMA

Angelcom S.A. se encuentra obligado a transmitir a TransMilenio S.A., de manera automática, la información del recaudo que TransMilenio S.A. requiera para su gestión operativa y para la fiscalización de la actividad de recaudo.

Partiendo de este punto, dada la evolución tecnológica para la operación de recaudo y su relación directa con los objetivos de la organización como lo menciona el manual de Calidad del Sistema de Gestión de Calidad de Angelcom S.A *“Proporcionar al cliente externo un sistema confiable, información oportuna, atención y soporte permanente” y su d*ependencia con el entorno, se podían presentar eventos no deseados internos o externos que comprometían el objetivo previamente mencionado, y por ende la protección de uno de los activos mas importantes; la información.

En su momento, la organización no tenía identificados los riesgos, amenazas y vulnerabilidades que a futuro afectarán la preservación de la disponibilidad, la confidencialidad e integridad de los sistemas de información. En conclusión, no existían suficientes controles para disminuir el impacto de los eventos no deseados; por lo que, ante su aparición, la organización solo podía manejarlos como “apaga fuegos”, La no adopción de buenas prácticas para el correcto manejo del riesgo; para el cumplimiento de los requerimientos contractuales, genera que no se garantice la veracidad de la información que se produce, como resultado de la explotación de la concesión de recaudo.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Diseñar el Sistema de Gestión de Seguridad de la Información en Angelcom S.A de tal manera que se evidencien los riesgos asociados a la información del sistema de recaudo.

1.2 .2 OBJETIVOS ESPECÍFICOS

1. Analizar y evaluar los riesgos a los que estaban sujetos los activos de la información de Angelcom S.A
2. Determinar el tratamiento de riesgos más adecuado para la mitigación del riesgo al interior de la organización.
3. Desarrollar un plan de continuidad del negocio concreto para la recuperación y el restablecimiento de los recursos y procesos de la organización.

1.3 JUSTIFICACIÓN

Angelcom S.A. es una empresa de ingeniería especializada en proyectos para la operación y mantenimiento de concesiones de transporte y control de acceso masivo, por ende las aplicaciones informáticas del sistema de recaudo debe contener según el contrato de concesión establecido entre Transmilenio S.A y Angelcom S.A lo siguiente: Administración de transacciones, generación de reportes, conciliación de transacciones, detección de fraude, Listas de medios de pago no válidos para el sistema, Monitoreo de problemas es decir gestión de incidentes, datos estadísticos de mantenimiento, administración de inventarios, módulo de seguridad y protección de la información; dichos requerimientos eran manejados, sin los debidos controles.

La organización en búsqueda de su mejoramiento continuo, quería establecer lineamientos que le permitieran ver los riesgos asociados a la seguridad de la información, entre los que incluyen robo de identidad, fuga de información, fraude y otros, por lo que era necesario contar con un marco de gobernabilidad en relación a la seguridad de la información; de esta forma, uno de los puntos más importantes para definir controles de seguridad de la información, era instaurar políticas claras al respecto, que establecieran un marco regulatorio para las actividades que debían ser llevadas a cabo en el diseño propuesto.

1.4 Diseño Metodológico

1.4.1 Tipo de Investigación

Las metodologías presentadas en el presente proyecto dentro de la óptica del ISO 27001, tienen una aplicación universal en cualquier organización, sin importar su tamaño, la industria a la que pertenecen o su naturaleza, bien sean empresas manufactureras o de servicios. Los métodos planteados son de fácil aplicación y permiten rápidamente que la organización se estructure de la manera correcta y más eficiente para implantar el diseño.

Para la realización del Diseño del Sistema de Gestión de Información se tomó como referencia la metodología establecida por el autor Alberto G. Alexander, con su libro “Diseño de un Sistema de Gestión de Seguridad de Información” por estar ajustada a las condiciones del objeto de estudio y las variables identificadas, y tener un enfoque orientado a las satisfacción de necesidades de información de la organización.

El autor de manera conceptualizada explica un patrón metodológico estratégico (funcional y flexible) para introducir gradualmente las etapas, para implantar un Sistema de Gestión de Seguridad de Información mediante un diseño fácil y estructurado, de tal forma que la organización obtenga como resultado un sistema eficaz y eficiente en todo su contexto.

Ésta metodología hace explícita la dependencia de todo el sistema de procesos con respecto a otros sistemas de gestión que la organización tenga implementado, el cual no permite la desviación del cumplimiento de los requisitos de cliente que en este caso es Transmilenio, y del cumplimiento de la visión, misión y objetivos estratégicos de la organización.

La presentación que hace referencia el autor, se encuentran influenciados por las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistema de soporte y la estructura de la organización.

Cada Diseño de un Sistema de Gestión de Seguridad de Información se confecciona de la manera más adecuada por tanto la consecución del presente estudio cuenta con la aplicación de un sistema de procesos, junto con la identificación e interacción de procesos, así como también de la gestión de la organización.

El modelo se baso en una investigación descriptiva la cual consistió en llegar a conocer las situaciones actuales y predominantes a través de la descripción exacta de las actividades, procesos y personas de Angelcom S.A. La predicción, la recolección de datos y la identificación de variables que se involucran en el desarrollo del estudio y su relación entre ellas “como variables dependientes: Los activos de información que darán el alcance del Diseño del Sistema de Gestión de Seguridad de la información. El análisis y evaluación del riesgo que se tomen alrededor de los activos de información identificados. Las amenazas que indiquen un evento potencial no deseado. Las vulnerabilidades que puedan hacer que una amenaza afecte un activo; y como variables independientes: los procesos que se identifiquen como críticos en el manejo de la información y la normatividad aplicable para la implementación del Sistema de Gestión de Seguridad de la Información;” permitieron que el estudio de caso tuviera un perspectiva de tipo deductivo para su desempeño y su perfeccionamiento en el tiempo. Este tipo de estudios conllevan a recoger información acerca de la situación existente de Angelcom S.A debido a su actividad económica y al gran llamado que tiene la organización en implementar el estándar ISO 27001:2005, y no simplemente es tomar la situación existente de la organización, sino también las experiencias y las condiciones pasadas que hacen parte del objeto de estudio.

El objetivo del presente estudio fue realizar una indagación a profundidad dentro de un marco de referencia como lo es la normatividad ISO 27001:2005, la cual tiene un enfoque de procesos basado en ciclo Deming Plan-Do-Check-Act; y basados en este ciclo, el Diseño del Sistema de Gestión de Seguridad de la Información se encuentra dentro de la primera etapa “Plan”.

Partiendo de estos puntos el ciclo metodológico para el Diseño del Sistema de Gestión de Seguridad de información que muestra el autor se ha validado en una serie de empresas en una variedad de industrias. Las fases del ciclo metodológico tienen un conjunto de actividades que se deben desarrollar en forma secuencial.

Bajo este lineamiento, el estudio reúne las condiciones metodológicas en razón que se utilizaron conocimientos sobre sistemas de gestión, a fin de aplicarlas en el proceso estratégico de la organización. Para este estudio se tuvo en cuenta un gran volumen de información que existe en lo perteneciente a las personas y hechos, debido a que la organización tiene implementado la norma ISO/9001:2008 Sistema de Gestión de Calidad; tales como:

- Documentación del SGC
- Caracterizaciones
- Mapa de Procesos
- Manual de Calidad
- Indicadores de control y gestión
- Planeación estratégica de la organización.
- Manual de perfiles

Facilitando el acceso y consulta de las fuentes de información de cada uno de los procesos que integran la organización. Otras fuentes importantes para el desarrollo del estudio, fueron los comités y/o reuniones que integraban

funcionarios de Angelcom S.A. con el fin de medir y evaluar la relación de variables dependientes. Para ello se realizaron entrevistas que generaron consensos definidos dentro de sus integrantes.

Se cuenta con diferentes instrumentos para la recolección de información, además de la medición de variables que se obtienen a partir del desarrollo del proyecto. Para dicho desarrollo se presenta la siguiente tabla donde se relaciona las fuentes, técnicas e instrumentos:

FUENTES, TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

VARIABLE	FUENTE	TECNICAS	INSTRUMENTOS
ACTIVOS DE INFORMACION	INFORMACION CORPORATIVA	ANALISIS DOCUMENTAL; ENTREVISTA	MÈTODO ELIPSES; ESCALA DE LIKERT
	DOCUMENTOS DE ESTRUCTURA FUNCIONAL Y ADMINISTRATIVA		
	MANUAL DE CALIDAD		
	DOCUMENTACION ESTRETEGICA DE LA ORGANIZACIÓN		
	FUENTES DOCUMENTALES DE ACCESO DE INFORMACION INTERNO Y EXTERNO		
	MEDIOS Y SISTEMAS DISPONIBLES		
	ANALISIS INFRAESTRUCTURA TECNOLOGICA		
	ACTIVOS DE SOFTWARE		
	ACTIVOS FISICOS		
	PERSONAL		
	CONTRATOS DE CONCESION		
ANALISIS Y EVALUACION DE RIESGO	IDENTIFICACION DE REQUERIMIENTOS LEGALES Y COMERCIA	ANALISIS DOCUMENTAL; ENTREVISTA	ESCALA DE RIESGOS;ESCALA DE LIKERT
	ASPECTOLEGAL		
	PRINCIPIOS,OBJETIVOS Y REQUERIMIENTOS PARA PROCESAI		
	IDENTIFICACION DE PERDIDAS CAUSADAS POR UN ACTIVO F		
	SENSIBILIDAD DE LOS DATOS Y EL SISTEMA		
AMENAZAS Y VULNERABILIDADES	LISTA DE VERIFICACION Y HERRAMIENTAS DE SOFTWARE	ANALISIS DOCUMENTAL	RELACION CAUSA Y EFECTO
	FUENTES DE AMENAZAS Y SU CAPACIDAD		
	NATURALEZA DE LA VULNERABILIDAD		

TABLA 3

Proceso Metodológico

Con el Sistema de Gestión de Seguridad de Información la organización pudo conocer los riesgos a los que está sometida la información del sistema de recaudo, asumiéndolos de tal manera que, se minimice, transfiera y controle mediante una sistemática definida, documentada y conocida por todos los miembros de la organización y mejore continuamente según las prioridades requeridas.

En un primer nivel de prioridad, el SGSI debe estar dirigido a la dirección de la organización y en un segundo nivel de prioridad, a la fuerza productiva y demás miembros y/o funcionarios de la organización; permitiendo de esta manera garantizar la gestión de la información confiable y oportuna que éstos necesitan para facilitar el proceso de toma de decisiones y desde luego permitir que las funciones de las diferentes áreas de la organización se realicen eficazmente.

El proyecto en mención hizo énfasis fundamentalmente en la detección de las fuentes, servicios y sistemas, como recursos informáticos y de los problemas subyacentes para obtener un inventario de los recursos y una serie de medidas para el mejoramiento de la gestión de la información de la organización.
Finalmente, la estructura del diseño estuvo compuesta por tres fases las cuales son determinantes para la ejecución del presente proyecto y de las cuales se mencionan a continuación:

FASE I: DETERMINACIÓN DEL ALCANCE DEL MODELO DEL SGSI.

La amplitud del alcance de Angelcom S.A. se determinará dependiendo de los recursos disponibles, la experiencia y la criticidad de los procesos en relación con los riesgos de información.

Definición del alcance obedece a dos parámetros: La primera es la estratégica, y la otra es la táctica, que es la netamente técnica; los cuales serán evidenciados en el diseño que es el objeto del presente proyecto.

FASE II: ANÁLISIS Y EVALUACIÓN DEL RIESGO.

En esta fase se identificaran aspectos como son los activos de información, comprendidos en el alcance del diseño del SGSI; seguidamente se valorará cada activo con base en la confidencialidad, integridad y disponibilidad. Una vez efectuada la tasación y/o valoración la organización decidirá que activos se consideran importantes para la continuidad del negocio.

A continuación se debe identificar y calcular las amenazas y vulnerabilidades para dar tratamiento a los riesgos e iniciar un proceso de toma de decisiones con respecto a cómo se tratará el riesgo, es decir; si los riesgos serán aceptados, transferidos o simplemente se evitarán.

FASE III: PCN "PLAN DE CONTINUIDAD DEL NEGOCIO"

El PCN significa en la organización, que se han identificado los procesos esenciales, se han determinado los tiempos de recuperación máximos tolerables, bajo los cuales estos procesos pueden estar paralizados sin colapsar el funcionamiento de la organización desde la perspectiva operacional y financiera.

ETAPA I: Business Impact Analysis (BIA)

Esta fase consiste en identificar aquellos procesos relacionados con apoyar la misión y visión de la organización, y analizar en detalle aquellos impactos en la

gestión del negocio, si esos procesos fuesen interrumpidos como resultado de una amenaza.

El entregable consiste en identificar las áreas de la organización que son críticas para el alcance de la planeación estratégica de la organización, así como la magnitud potencial del impacto operativo y financiero de una interrupción en el desempeño de la organización y por ende en el cumplimiento de los requerimientos contractuales del ente gestor.

ETAPA II: Gestión del riesgo.

Las actividades de gestión del riesgo evalúan las amenazas de un desastre, pormenorizan las vulnerabilidades existentes, los potenciales impactos, se identifican los controles necesarios para prevenir los riesgos y se termina identificando escenarios de amenazas para aquellos procesos considerados como críticos en el BIA.

El entregable de esta etapa es la identificación de riesgos y controles y posibles amenazas potenciales de interrupciones del negocio y los respectivos riesgos; puntualizando de tal manera que evidencie las alteraciones del normal desempeño de los procesos de la organización.

Para la gestión del riesgo se tomará como base los siguientes parámetros:

1. Identificación de amenazas
2. Identificación de vulnerabilidades
3. Revisión de controles actuales
4. Cálculo del nivel de exposición del riesgo

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo cual es necesario que toda organización que busque una excelencia en los servicios o productos que ofrece, adopte una Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. Toda organización que desee convertirse en un proveedor confiable debería garantizar la continuidad de su negocio ante posibles escenarios de amenazas.

En línea con estos propósitos, el estándar ISO/IEC 17799 se ha convertido en una referencia para la comunidad internacional con respecto a la gestión de la seguridad de la información.

ISO/IEC 17799 es de alto nivel, amplia en su alcance, y conceptual en su naturaleza. Este enfoque le permite ser aplicada a múltiples tipos de empresas y aplicaciones. También se ha hecho polémica entre aquéllos que creen que las normas deben ser lo más precisas posibles. A pesar de esta controversia, ISO 17799 es el único “Standard” consagrado a la Gestión de Seguridad de Información en un campo generalmente gobernado por las “Pautas, las Guías” y “las Mejores Prácticas.”

ISO/IEC 17799 define la información como un recurso que puede existir en muchas formas y puede tener un valor para una organización. La meta de la seguridad de información es proteger este recurso adecuadamente para asegurar la continuidad comercial y operativa, minimizar el daño comercial, y aumentar al máximo el retorno en las inversiones. Como esta definido por ISO/IEC 17799, la seguridad de la información se caracteriza como la preservación de:

- La Confidencialidad de la información, asegurando esa información para que sólo sea accesible a aquéllos autorizados a tener el acceso.
- La Integridad y autenticidad salvaguardando la exactitud e integridad de información y métodos de procesamiento.
- La Disponibilidad, asegurando a los usuarios autorizados el acceso a la información y a los recursos asociados cuando los requiere.

Diferentes naciones han reconocido la importancia del tema y promovido un ambiente a favor de la confidencialidad, integridad, disponibilidad y autenticidad de la información, considerada un bien de importancia estratégica en el desarrollo económico y social.

La norma BS 7799 y el BSI han estado mucho tiempo proactivos en la arena de la evolución de la Seguridad de la Información. En respuesta a las exigencias de la industria, un grupo activo consagrado a la Seguridad de la Información se estableció como pionero en el año 990, en Inglaterra culminando en 1993 un "Código de Práctica para Gestión de la Seguridad de Información". Este trabajo evolucionó en la primera versión de la norma de 7799 que el BSI emitió en 1995.

Al final del año 1990 en respuesta otra vez a requerimientos de la industria, el BSI formó un programa para acreditar a las empresas, ("los Cuerpos de la Certificación,") como competentes para operar bajo la norma BS 7799. Este esquema es conocido como el cure simultáneamente, un comité directivo se formó, mientras se culminó con la actualización y emisión de BS 7799 en 1998 por primera vez y después en 1999 la segunda edición. La norma BS 7799 actual consiste de:

- Parte 1: El código de Práctica, y
- Parte 2: La especificación de un Sistema de Gestión para la Seguridad de Información

Por este tiempo, la seguridad de información se había vuelto noticia del titular de los periódicos y una preocupación de los usuarios de la computadora a nivel mundial. Mientras algunas organizaciones utilizaron el BS 7799 normal, la

demanda creció por una norma seguridad de la información internacionalmente reconocida bajo el amparo de un cuerpo o institución internacionalmente reconocida, como el ISO. Esta demanda llevó al “arrastre rápido” de BS 7799 Parte 1 por el BSI, culminando en su primera edición por ISO como ISO/IEC 17799:2000 en el 2000 de diciembre.

A partir de Septiembre del 2001, sólo BS 7799 Parte 1 se ha aceptado para la estandarización de ISO porque es aplicable internacionalmente y por todos los tipos de organizaciones. EI intento para someter BS 7799 Parte 2 a una estandarización de ISO ha sido suspendido.

El ISO/IEC JTC 1/SC 27 viene desarrollando una familia de Estándares Internacionales para el Sistema de Gestión de Seguridad de la Información (ISMS). La familia incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. La familia adoptará el esquema de numeración utilizando las series del número 27000 en secuencia.

Para cubrir estas necesidades la ISO -Organización Internacional para la Estandarización- creó una norma certificable que permite a las organizaciones encaminarse en un Sistema de Gestión de Seguridad de la Información, la ISO 27001.

Para el cumplimiento de las directrices de la norma ISO/IEC 27001, las organizaciones deben cumplir los numerales 4 al 8 descritos en la norma, los cuales hacen referencia a: requisitos generales, establecimiento del SGSI, implementación y operación del SGSI, seguimiento y revisión del SGSI, mantenimiento y mejora del SGSI, requisitos de documentación exigidos por la norma, responsabilidad de la dirección, gestión de los recursos, auditorias internas, revisión por la dirección y mejora continua del SGSI.

Adicionalmente las organizaciones deben implementar los objetivos de control y los controles descritos en los numerales 5 al 15 de la ISO/IEC 27002, que cumplan

los requisitos identificados en el proceso de valoración y tratamiento de riesgos.

¿Qué es un Sistema de Gestión de Mejora Continua? según el British Standard Institute es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Las empresas que operan en el siglo XXI se enfrentan a muchos retos, significativos, entre ellos: Rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento y tecnología. Equilibrar estos y otros requisitos empresariales puede constituir un proceso difícil y desalentador. Es aquí donde entran en juego los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización.

La implementación de un sistema de gestión eficaz puede ayudar a:

- Gestionar los riesgos sociales, medioambientales y financieros.
- Mejorar la efectividad operativa.
- Reducir costos.
- Aumentar la satisfacción de clientes y partes interesadas.
- Proteger la marca y la reputación.
- Lograr mejoras continuas.
- Potenciar la innovación.
- Eliminar las barreras al comercio.
- Aportar claridad al mercado.

El uso de un sistema de gestión aprobado le permite renovar constantemente su objetivo, sus estrategias, sus operaciones y niveles de servicio.

La norma ISO/IEC 27001 es la normativa certificable para los Sistemas de Gestión

de Seguridad de la Información, la cual evolucionó del estándar ISO 17799 que a su vez se derivó de la BS 7799. La BS 7799 es una norma que presenta los requisitos para un Sistema Administrativo de Seguridad de la Información (SASI). Ayudará a identificar, administrar y minimizar la gama de amenazas a las cuales está expuesta regularmente la información

La metodología de los Sistemas de Gestión se basa en el Ciclo Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, cuyas pasos son: Planear, Implantar, Revisar y Mejorar o PLAN-DO-CHECK-ACT (PDCA). La representación gráfica del ciclo de Deming abstrae el concepto de mejora continua por la retroalimentación del paso final al paso inicial.

Las cláusulas de la norma se distribuyen usando como base el ciclo en mención cuya adopción operativa en la organización, constituye un factor clave para el Sistema de Gestión de Seguridad de la información (SGSI) o Information Security Management System (ISMS) por sus siglas en inglés

La metodología de implantación debe desarrollarse acorde a las cláusulas 4.2 descrita en la Norma ISO 27001 correspondiente al establecimiento y operación de SGSI. La misma que nos indica que debemos definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de la justificación de cualquier exclusión del alcance.

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto. También se acostumbra , para la toma de decisiones coyunturales, constituir un comité de seguridad liderado por el Director o Gerente General y conformado por Gerencias de diferentes áreas como la de tecnología, financiera, Recursos Humanos, Comercial, operaciones, etc.

La cláusula 4.2.1 de la norma también nos indica que debemos establecer una

política de seguridad de la información acorde a las características del negocio, organización, activos, regulaciones y tecnología. Es muy poco exacto redactar una política de seguridad para toda la organización al iniciar el proceso de implantación, la buena práctica es redactarla en paralelo al proceso de acuerdo a las necesidades del sistema, que irán apareciendo. Lo que se recomienda es redactar una Política de Seguridad de Información general que guíe lo que queremos conseguir mediante nuestro SGSI.

Adicionalmente a la norma ISO/IEC 27001, existen otros estándares de los cuales hacen parte de las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener los Sistemas de Gestión de Seguridad de la Información (SGGI) tales como:

ISO/IEC 27002: Está en fase de desarrollo, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, esta norma no es certificable

ISO/IEC 27003: Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA ((Plan-Do-Check-Act:).Tomado del ciclo de calidad de Edwards Deming)) y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2.

ISO/IEC 27004: Publicada probablemente en Noviembre de 2006. Especificará las métricas y técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO/IEC 27005: Consiste en una guía para la gestión del riesgo de la seguridad de la información y servirá de apoyo a la ISO 27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en Marzo de 2006) y, probablemente, en ISO 13335.

ISO/IEC 27006: Especificará el proceso de acreditación de entidades de certificación y el registro de SGSI.

Las políticas y los procedimientos de seguridad informática surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización. Deben considerarse como reglas a cumplir que surgen para evitar problemas y que se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.

Un plan de seguridad en una organización debe estar soportado por políticas y procedimientos que definan el porque proteger un recurso, que quiere hacer la organización para protegerlo y como debe procederse para poder lograrlo.
Una de los aspectos más importantes que se debe considerar, en el desarrollo de políticas de seguridad, es poder determinar qué es lo que se quiere proteger y de qué se quiere proteger. Para lograr esto es importante tener conocimiento de las vulnerabilidades y formas de ataque de los sistemas con que cuenta la organización. Los ataques internos los pueden realizar personas con buen conocimiento de técnicas para acceder a cuentas a las que no están autorizados o pueden surgir como accidentes que se presentan por el mal uso de los recursos.

Los ataques externos provienen de personas experimentadas en acceder a los sistemas a través de las diferentes modalidades de conexión a redes internas.
En general estas personas poseen buenos conocimientos sobre Software, Hardware, programación, lenguaje ensamblador, sistemas operativos, TCP/IP, protocolos de seguridad, etc.

2.2 MARCO CONCEPTUAL

¿Qué es seguridad de la información?

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente.

Como resultado de ésta creciente ínter conectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

¿Por qué se necesita seguridad de la información?

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante para proteger las infraestructuras críticas tanto para negocios del sector público como privado. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.
Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

Punto de inicio de la seguridad de la información

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en

requerimientos legislativos esenciales o pueden ser considerados como una práctica común para la seguridad de la información.
Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a. Protección de data y privacidad de la información personal.
b. Protección de los registros organizacionales.
c. Derechos de propiedad intelectual.

- Los controles considerados práctica común para la seguridad de la información incluyen:

a. Documento de la política de seguridad de la información.
b. Asignación de responsabilidades de la seguridad de la información.
c. Conocimiento, educación y capacitación en seguridad de la información.
d. Procesamiento correcto en las aplicaciones.
e. Gestión de la vulnerabilidad técnica.
f. Gestión de la continuidad comercial.
g. Gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en este estándar son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

Desarrollo de sus propios lineamientos

Este código de práctica puede ser visto como un punto de inicio para desarrollar los lineamientos específicos de la organización. No todos los controles y lineamientos en este código de práctica pueden ser aplicables. Es más, se pueden requerir controles y lineamientos adicionales no incluidos en este estándar. Cuando los documentos son desarrollados conteniendo lineamientos o controles adicionales, cuando sea aplicable podría ser útil incluir referencias cruzadas con las cláusulas en este estándar para facilitar el chequeo de conformidad realizado por los auditores y socios comerciales.

Identificación los procesos.

La identificación de procesos dentro del alcance constituye un pilar fundamental para el enfoque del SGSI. En nuestro caso los procesos involucrados son: Monitoreo, Control de cambios, mantenimiento y aprovisionamiento.
Para una organización donde no exista una cultura de procesos o simplemente no se los tiene identificado es recomendable primero realizar un correcto levantamiento de procesos antes de avanzar con la implantación del SGSI.

Métodos de las elipses.

El método de las elipses es un mecanismo que permite identificar dentro de un proceso todas las relaciones de sus subprocesos y actividades con otras áreas de la organización, y entidades externas. Una vez establecidas las relaciones es casi natural poder identificar los activos de información que se usan en dicha relaciones.

Identificación y tasación de activos.

Los activos de información pueden ser el software, el hardware, los enlaces, el equipamiento, los documentos, las personas que manejen (Procesen, trasladen, almacenen) información de valor para el negocio de la organización. El proceso de tasación de activo también es recomendado hacerlo mediante un taller multidisciplinario.

Las relaciones encontradas mediante el método de las elipses nos permitieron visualizar con claridad los activos involucrados. El siguiente paso es tasar el listado de los activos para quedarnos con aquellos de mayor valor. La pregunta para evaluar es ¿la pérdida o deterioro de este activo, cómo afecta la disponibilidad, confidencialidad e integridad del proceso del negocio de la compañía? , en nuestro caso se usó la escala de 1 a 5, siendo el 1 de menor afectación y 5 de mayor afectación. El valor total del activo es el promedio entero de los valores asignados a la disponibilidad, confidencialidad e integridad. Una vez calculado el valor por cada activo, seleccionamos aquellos de mayor valor. El valor umbral queda a discreción de cada organización por ejemplo serán de importancia aquellos con un valor mayor a 3.

Factores de éxito críticos

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

- Política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales;
- Un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;

- Soporte visible y compromiso de todos los niveles de gestión;
- Un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;
- Marketing efectivo de la seguridad de la información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema;
- Distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas;
- Provisión para el financiamiento de las actividades de gestión de la seguridad de la información;
- Proveer el conocimiento, capacitación y educación apropiados;
- Establecer un proceso de gestión de incidentes de seguridad de la información;
- Implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

EVALUACIÓN Y TRATAMIENTO DEL RIESGO

Evaluación de los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).
Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva e incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.
El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Lineamientos para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad TI).

Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a. Aplicar los controles apropiados para reducir los riesgos;
b. Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;
c. Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;
d. Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo.

Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

- Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:
- Objetivos organizacionales;
- Requerimientos y restricciones operacionales;
- Costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;
- La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización.

Cada uno de los procesos operativos de Angelcom S.A., define como está asociado a los requerimientos exigidos contractualmente y a los requerimientos propios, contemplados por la organización y con base en esto se define e implementa un Sistema de gestión de calidad que soporta la operación de los procesos y por ende sus actividades bajo la realización, verificación y control.

La organización tiene definido las características funcionales de los equipos y del software con el fin de garantizar que el producto resultante cumpla con los requerimientos especificados por el cliente; pero no tiene definido los riesgos y controles que se deben de tomar en cuanto a la seguridad de información; se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
• **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de

negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Al referirse específicamente al concesionario; el Sistema debe contar con rutinas de verificación de integridad de la información. Los errores detectados deberán ser corregidos automáticamente para impedir la propagación de datos inválidos a lo largo de la base de datos. Las transacciones duplicadas o incompletas se deberán detectar y corregir sin que ello implique una detención total del Sistema. En el caso de una transacción incompleta o de interrupciones en la comunicación la parte del sistema afectada deberá reparar y registrar inmediatamente el error; para así dar cumplimiento a los requerimientos contractuales adecuadamente.

[2]Para propósitos de este documento, se aplican los siguientes términos y definiciones.

- **Activo**

  Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004)

- **Control**

---

[2] ESTÁNDAR INTERNACIONAL ISO/IEC 17799 Tecnología de la Información – Técnicas de seguridad – -Definiciones- Código para la práctica de la gestión de la seguridad de la información.

Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

- **Lineamiento**

Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas (ISO/IEC 13335-1:2004)

- **Medios de procesamiento de la información**

Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

- **Seguridad de la información:**

Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad y confiabilidad.

- **Evento de seguridad de la información**

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC TR 18044:2004)

- **Incidente de seguridad de la información**

Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (ISO/IEC TR 18044:2004).

- **Política**

Intención y dirección general expresada formalmente por la gerencia.

- **Riesgo**

Combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC Guía 73:2002).

- **Análisis del riesgo**

Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

- **Evaluación del riesgo**

Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo (ISO/IEC Guía 73: 2002).

- **Gestión del riesgo**

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

NOTA. La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. (ISO/IEC Guía 73: 2002).

- **Tratamiento del riesgo**

Proceso de selección e implementación de medidas para modificar el riesgo. (ISO/IEC Guía73: 2002).

- **Amenaza**

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004).

- **Vulnerabilidad**

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 13335-1:2004).

2.3 MARCO LEGAL

Para el desarrollo del Diseño del Sistema de Gestión de Seguridad de Información se tuvo en cuenta la siguiente:

2.3.1 Normatividad

Estándares internacionales a considerar tales como:

- **ISO/IEC 17799:2005**

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización.
Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

- **COBIT**

Acrónimo de “Control Objectives for Information and related Technology” (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y 239 conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos 5

años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC.

- **ITIL**

Acrónimo de “Information Technology Infrastructure Library”, ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

- **LEY SOX**

La Ley Sarbanes-Oxley (SOX), de EE.UU., nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la Securities and Exchange Comission a llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como Enron y Worldcom, durante el año 2002, en los cuales se comprobó que información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que transan sus valores en la bolsa de EE.UU.

- **COSO**

La normativa COSO, acrónimo de The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. Junto a esto son muchas otras las

normas que están directa o indirectamente relacionadas con ésta como por ejemplo COBIT.
En síntesis, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

- **ISO Serie 27000**

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI
(Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) [6] (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799)

2.3.2 LEGAL

En los últimos años se han perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de la información, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales e internacionales.
La ONU señala que cuando el problema se eleva e la escena internacional, se magnifican los inconvenientes y los delitos informáticos se constituyen en una forma de crimen transnacional.

LEGISLACIÓN NACIONAL

- Ley 599 de 2000 Código Penal - Artículos 195, 240, 247, 270,271, 272
- Ley 1273 de 2009.

El 5 de Enero de 2009 el Congreso de la Republica de Colombia, promulgo la ley 1273 “por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado – “De la protección de la Información y de los datos” – y se preservan integralmente los sistemas de utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.
Dicha ley tipifico como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de computo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez mas usuales en todas partes del mundo. Según la revista Cara y Sello,

durante el 2007 en Colombia las empresas perdieron mas de 6.6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona el Código Penal Colombiano el titulo VII BIS denominado “De la protección de la Información y de los datos” que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y de los “Atentados Informáticos y otras infracciones”

- Ley 527 de 1999, Comercio electrónico
- Ley 906 Código de Procedimiento Penal Artículos 235,236,275
- Contrato de concesión para el recaudo en el Sistema Transmilenio.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, España, Argentina y Chile entre otros. Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

- **Estados Unidos**. Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.
- **Alemania**: Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:
  * Espionaje de datos.
  * Estafa informática.
  * Alteración de datos.
  * Sabotaje informático.
- **España**: En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa.
- **Chile**: Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

3 RESULTADOS

ANGELCOM S.A es una empresa de ingeniería especializada en proyectos para la operación y mantenimiento de concesiones de transporte y control de acceso masivo, incursionó en el campo de los sistemas de recaudo al introducir la tecnología de la Tarjeta Inteligente sin contacto (TISC) en el proyecto Transmilenio, lo que hizo que transformara sus operaciones y se dedicara exclusivamente a operar y mantener sistemas de recaudo Con lo anterior, se puede resumir en la figura 1 la operación de Angelcom S.A identificando los puntos críticos de información que actualmente se maneja.

DIAGRAMA DE OPERACIONES DE ANGELCOM S.A

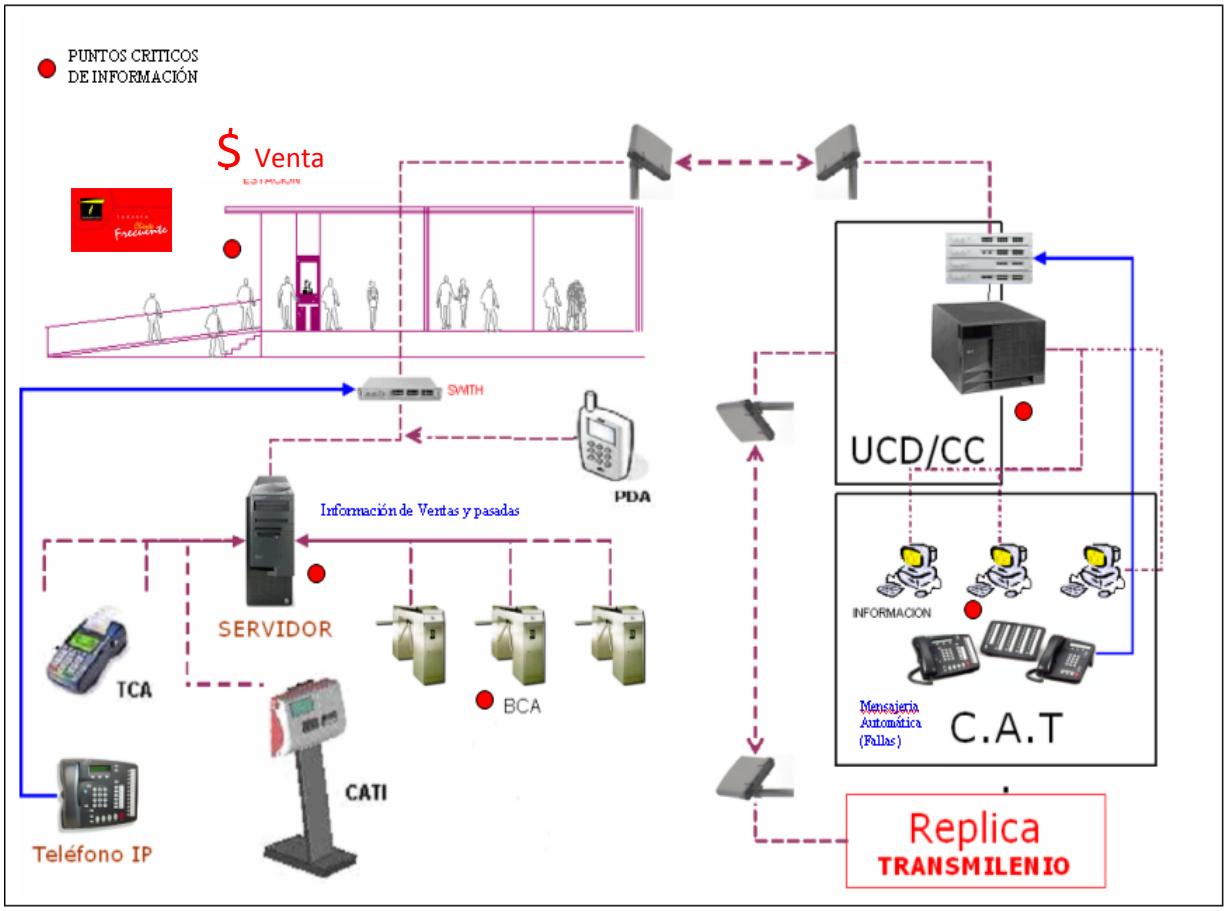

FIGURA 1.

ANÁLISIS Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

FASE I: DETERMINACIÓN DEL ALCANCE DEL MODELO DEL SGSI.

En esta etapa se identificaron los “factores críticos del éxito” de la organización y, por otro lado, los procesos críticos en donde se dirigió a resolver la siguiente pregunta: ¿Cuál o cuales procesos son críticos y afecten la seguridad de la información?

Los factores críticos del éxito se entienden como aquellas características organizacionales de quien depende el éxito o fracaso de la empresa; para esto se tuvo en cuenta lo estipulado en la norma ISO/IEC 13335-1:2005 y en la norma ISO/IEC 17799:2005. Estas normatividades permitieron alinear dichos factores con la actividad propia de la organización y por ende a la estructura del Sistema de Gestión de Calidad establecido durante 6 años por la organización según documento CA-MA-P-001 MANUAL DE CALIDAD DEL SGC, dando como resultado los siguientes factores:

- Cumplimiento a los requerimientos contractuales
- Excelencia en la operación
- Empleados competentes
- Satisfacción del cliente
- Nuevas oportunidades de negocio
- Costos competitivos.

Para identificar los procesos de la organización que tienen mayor impacto dentro de los factores críticos del éxito, se verifico el mapa de procesos y las caracterizaciones de cada proceso y su debida interacción, con el fin de tener un criterio valido y documentado sobre la siguiente matriz titulada “Matriz de despliegue del Sistema de Gestión de Seguridad de la Información”

MAPA DE PROCESOS DE ANGELCOM S.A.

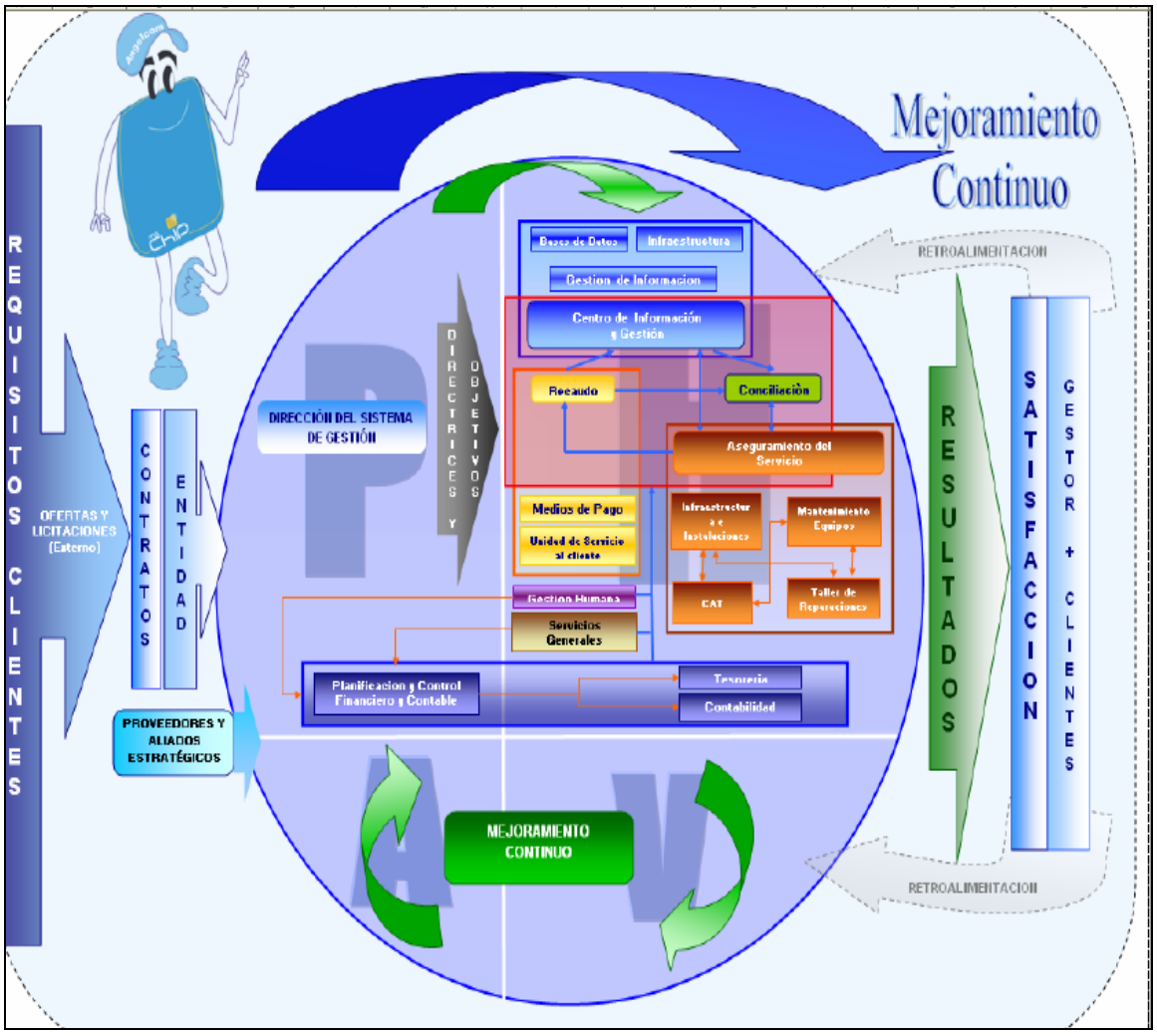

FIGURA 2.

Fuente: CA-P-001 Manual de Calidad de Angelcom S.A

Las caracterizaciones de los procesos se encuentran como anexos para su verificación, según formato CA-MA-002 CARACTERIZACIONES. Ver Anexo 1.

Por otro lado; después de verificar la información anteriormente relacionada se confirmo con cada líder de proceso el impacto que tiene cada proceso frente a los factores críticos de éxito que serán determinantes a la hora de realizar el alcance del Sistema de Gestión de Seguridad de la Información.

Para esta actividad se realizo una pequeña encuesta con el fin de conocer estados de opinión, características o hechos específicos. La amplitud del alcance de la organización dependió de muchos factores, unos de ellos fueron los recursos disponibles, la experiencia en la operación de recaudo y la criticidad de los procesos que fueron identificados y que impactaron en el riesgo de la información de la organización.

El propósito de la matriz fue identificar aquellos procesos de la organización con mayor impacto, los cuales serian los candidatos para tomar en cuenta para la definición del alcance del Diseño del Sistema de Gestión de Seguridad de la Información. Para esta matriz, se hizo uso de la escala de Likert la cual mide todos los escenarios o disposiciones individuales en contextos sociales particulares; se le conoce también como la escala sumada debido a que la puntuación de cada unidad de análisis se obtiene mediante la sumatoria de los criterios establecidos en cada ítem.

La escala se construye en función de una serie de ítems que reflejan una actitud y/o comportamiento acerca de un referente. Cada ítem esta estructurado con cinco alternativas de respuesta tal como se muestra en la tabla 3,

ESCALA DE LIKERT.

CRITERIO	ESCALA DE CALIFICACION		
NO TIENE IMPACTO	0	A	0
IMPACTO LEVE	0	A	2
IMPACTO MEDIO CONTROLABLE	2	A	4
IMPACTO GRAVE CONTROLABLE	4	A	6
IMPACTO GRAVE NO CONTROLABLE	6	A	màs

TABLA 4

Fuente: www.eumed.net/libros/introduccionalametodologiadelainformacion

Bajo este esquema se realizo la etapa estratégica como se puede evidenciar en la tabla 5. En seguida, a los procesos considerados críticos, se les determinó su grado de criticidad en relación con su exposición al riesgo de información.

ETAPA ESTRATÉGICA

MATRIZ DE DESPLIEGUE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”

- GERENCIA DE ADMINISTRATIVA Y FINANCIERA
- GERENCIA DE OPERACIONES

FACTORES CRITICOS DEL ÉXITO	CUMPLIMIENTO A REQUERIMIENTOS CONTRACTUALES	EXCELENCIA EN LA OPERACIÓN	EMPLEADOS COMPETENTES	SATISFACCION DEL CLIENTE	NUEVAS OPORTUNIDADES DE NEGOCIO	COSTOS COMPETITIVOS	TOTAL
PROCESOS DE LA ORGANIZACIÓN							
DIRECCION ASEGURAMIENTO DEL SERVICIO							**17**
MANTENIMIENTO DE EQUIPOS	x	x	x	x		x	5
TALLER DE REPARACIONES	x	x	x	x		x	5
CENTRO DE ASISTENCIA TECNICA	x	x	x	x			4
INFRAESTRUCTURA E INSTALACIONES	x		x			x	3
DIRECCION RECAUDO							**10**
RECAUDO		x	x	x			3
SERVICIO AL CLIENTE			x	x			2
MEDIOS DE PAGO			x	x			2
CONCILIACION	x	x		x			3
DIRECCION CENTRO DE INFORMACION Y GESTION							**15**
BASE DE DATOS	x	x	x	x		x	5
INFRAESTRUCTURA	x	x	x	x		x	5
GESTION DE INFORMACION	x	x	x	x		x	5
PLANIFICACION Y CONTROL FINANCIERO Y CONTABLE							**4**
CONTABILIDAD					x		1
TESORERIA					x		1
PLANEACION FINANCIERA	x				x		2
GESTION HUMANA			x	x		x	**3**
SERVICIOS GENERALES		x		x		x	**3**
MEJORAMIENTO CONTINUO			x				**1**

TABLA 5.

Fuente: Mapa de Procesos de Angelcom S.A. Normas ISO/IEC 13335-1:2005 y ISO/IEC 17799:2005

De acuerdo a la escala y seguidamente a los resultados obtenidos en la matriz; se puede constatar que los procesos mas críticos a nivel organizacional son: Aseguramiento del Servicio y Centro de Información y Gestión,. Para mayor comprensión se tomo como base de la estadística descriptiva la media aritmética expresada en la cantidad total de la variable distribuida a partes iguales entre cada observación; lo que permitió analizar y representar los datos generados por la escala de calificación y de acuerdo a la matriz mencionada en la tabla 5. Dando como resultado que el 35% de todos los procesos y/o subprocesos de la organización se encontraban dentro de un impacto grave controlable, a comparación de los demás procesos.

Con la información consignada se identificaron los procesos que se les realizaría la etapa táctica; la cual consiste en aplicar la etapa estratégica, la “metodología de las elipses”.

Este método permitió identificar con gran detalle los componentes de cada proceso y las interfaces con otros procesos en la organización y con entidades externas a ella. Por lo tanto; el método de las elipses cuenta con el siguiente esquema, siendo este último un método fácil y sencillo para visualizar gráficamente sus interacciones con la información:

Lo primero que se hizo fue determinar en la elipse concéntrica los distintos subprocesos que conforman el proceso de Aseguramiento del Servicio y Centro de Información y Gestión. El segundo paso, consistió en identificar en la elipse intermedia las distintas interacciones que los subprocesos de la elipse concéntrica tienen con otros procesos de la organización. Seguidamente, en la elipse externa, se identificaron aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse concéntrica. Las flechas indican el tipo de interacción, y la direccionalidad que tiene el flujo de información.

ETAPA TÁCTICA:

METODOLOGÍA DE LAS ELIPSES PARA ASEGURAMIENTO DEL SERVICIO

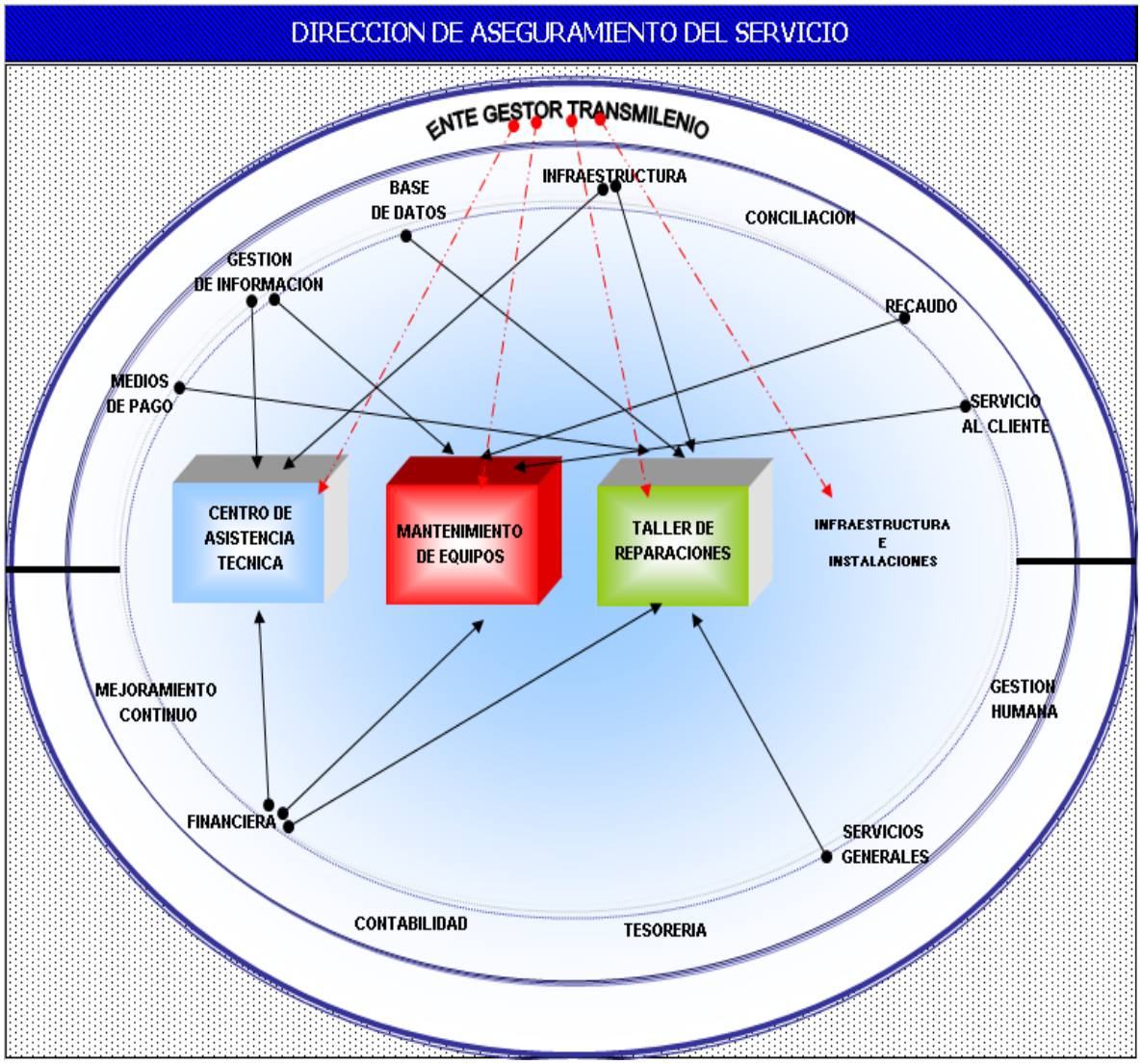

FIGURA 3.

Fuente: Alberto G. Alexander. Óptica ISO 27001:2005

METODOLOGÍA DE LAS ELIPSES PARA CENTRO DE INFORMACIÓN Y GESTIÓN

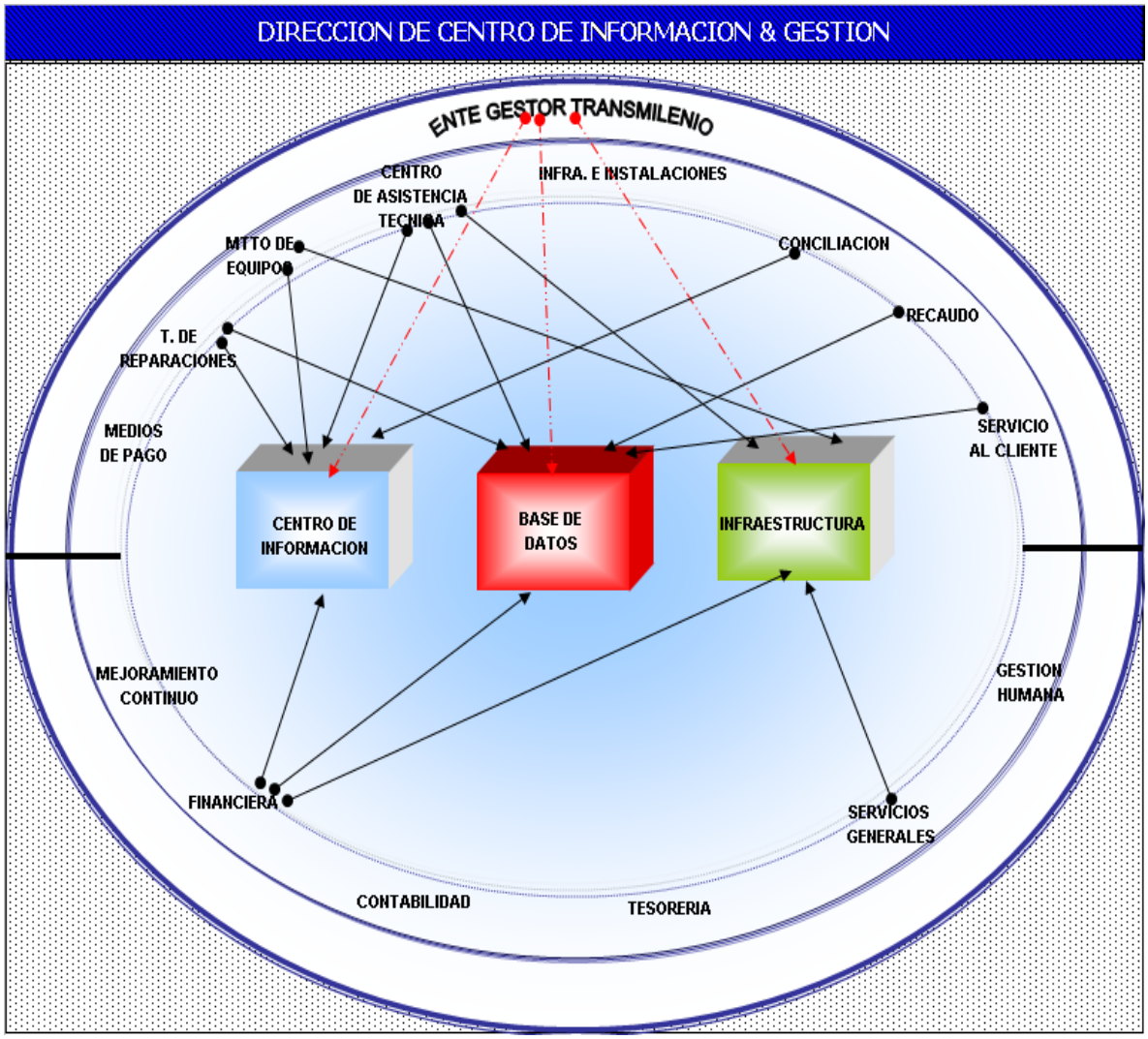

FIGURA 4

Fuente: Alberto G. Alexander. Óptica ISO 27001:2005

ALCANCE Y POLÍTICA DEL SGSI DE ANGELCOM S.A.

DISEÑO DEL SISTEMA DE GESTIÓN

DE SEGURIDAD DE LA INFORMACIÓN

ALCANCE:

El Sistema de Gestión de Seguridad de la Información de Angelcom S.A. aplica a todas las actividades de operación y mantenimiento del sistema de recaudo para concesiones de transporte y control de acceso masivo; y aquellos procesos críticos tales como Aseguramiento del Servicio y Centro de Información y Gestión, para proveer la seguridad de la información de los activos de la organización y de la PTR en lo perteneciente a (Hardware, Software y Comunicaciones); dando cumplimiento a los requerimientos de seguridad determinados en la evaluación del riesgo y por los requerimientos regulatorios establecidos de tal manera que generen confianza a los clientes y a las partes interesadas.

POLÍTICA SGSI:

Todo el personal de Angelcom S.A. en lo perteneciente a la seguridad de la información relacionada con la operación del sistema de recaudo y mediante el mejoramiento continuo se comprometa a:

- Asegurar que los usuarios autorizados tengan los accesos a la información de los procesos, sistemas y redes que la soportan.
- Preservar la veracidad y completitud de la información y los métodos de procesamiento.
- Asegurar que la información solo sea accedida de manera segura, de forma que permanezca protegida de pérdidas, manipulaciones o divulgaciones no autorizadas.
- Incrementar la seguridad de los activos de información pertenecientes a (Hardware, Software y Comunicaciones).
- Asegurar los controles establecidos por la norma ISO/IEC 27001:2005.

TABLA 6.

FASE II: ANÁLISIS Y EVALUACIÓN DEL RIESGO.

Para dar inicio al Análisis y evaluación del riesgo; primeramente se realizó el inventario de los activos de toda la información necesaria para poder determinar la recuperación de un posible desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.
Basados en la importancia del activo, su valor comercial y su clasificación de seguridad, se tomó como guía la clasificación de activos que la norma ISO/IEC 17799:2005 determina:

- **Información:** bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoria e información archivada.
- **Activos de software:** software de aplicación, software del sistema, herramientas de desarrollo y utilidades;
- **Activos físicos:** equipo de cómputo, equipo de comunicación, medios removibles y otro equipo;
- **Servicios:** servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;
- **Personas**, y sus calificaciones, capacidades y experiencia;
- **Intangibles**, tales como la reputación y la imagen de la organización.

En esta fase se identificaron los activos de información de cada uno de los procesos críticos, mediante la verificación actual de la documentación del SGC; y mediante la recolección de datos de los procesos involucrados para así determinar que tipo de activos de acuerdo a su clasificación eran aplicables o no dentro del Diseño del Sistema de Gestión de Seguridad de la Información. La recolección de datos se realizó, teniendo en cuenta la interacción dada en las figuras 3 y 4 del presente documento, y dado los requisitos contractuales del ente gestor.

Por consiguiente, se dio inicio a la valoración de cada activo con base en la confidencialidad, integridad y disponibilidad; según los lineamientos dados por la norma ISO/IEC TR 13335-3. Una vez efectuada la tasación y/o valoración la organización se pudo decidir que activos se consideran importantes para la continuidad del negocio.

1. IDENTIFICACIÓN DE ACTIVOS

A continuación se relacionan los activos de información identificados en cada uno de los procesos críticos:

ACTIVOS DE INFORMACIÓN ASEGURAMIENTO DEL SERVICIO

ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos
		Incidencias Operativas
		Configuraciòn dispositivos de memoria
		Versiones de Firmware
		Actualización remota
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso
		Entregas de obras Transmilenio
		Contrato de concesion
		Especificaciones tecnicas de equipos
	ACTIVOS DE SOFTWARE	Windows NT
		Linux
		Faxila
		Ovunto
		NSM
		Service Desk
		Intranet
		Putty
	ACTIVOS FISICOS	Equipos de configuracion
		Equipos de recaudo
		Servidores
		Banco de pruebas
	PERSONAL	Auxiliar de Mantenimiento de equipos
		Auxiliar Administrativa de activos
		Auxiliar de Mantenimiento Almacen Satelite

TABLA 7.

Fuente: norma ISO/IEC 17799:2005

ACTIVOS DE INFORMACIÓN CENTRO DE INFORMACIÓN Y GESTIÓN

CENTRO DE INFORMACION Y GESTION	**ACTIVOS DE INFORMACION**	Base de datos estaciones
		Base de datos transacciones
		Base de datos pasadas
		Versiones de Software
		Base de datos usuarios
		Desencole dispositivos de almacenamiento
		Protocolos IP de equipos de recaudo
		Protocolos IP de equipos de computo
		Acceso remoto
		Listas negras
		Listas blancas
	DOCUMENTOS DE PAPEL	Protocolos de software
		Bitacoras de acceso Centro de Computo
		Certificado digital
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication
		ServiceDev
		Toad
		Protocolo TCP/IP
		Batch
		VNP
		VNC
		Unicenter
	ACTIVOS FISICOS	Centro de computo
		Servidor de archivos de la organización
		Servidor base de datos
		UCD¨s (Unidad central de datos)
		Router¨s
		Switchers
		Modulos SAM Llaves de seguridad
		Servidor NSM
		Servidor SD
		Controlador de Dominio
	PERSONAL	Analista de Sistemas
		Tecnico de Sistemas
		Auxiliar de Soporte
		Administrador Base de datos
		Operario de Informatica

TABLA 8.

Fuente: norma ISO/IEC 17799:2005

2. IDENTIFICACIÓN DE REQUERIMIENTOS LEGALES Y COMERCIALES RELEVANTES PARA LOS ACTIVOS IDENTIFICADOS

Los requerimientos de seguridad para Angelcom S.A;, se derivan de 2 fuentes:

- Aspecto legal: Requerimientos contractuales.
- Conjunto de operaciones que la organización ha desarrollado.

Dentro de los aspectos legales y las operación propias, que la organización ha desarrollado, se tuvo en cuenta el nivel de cumplimiento según los ítems abajo mencionados y los controles actuales y los que definitivamente no existen dentro de la operación de recaudo. En la tabla 9 se puede evidenciar lo mencionado con anterioridad; dicha información se tomo del Contrato de Concesión y se creo un Comité, en las que intervinieron los siguientes funcionarios:

a. Asesor Jurídico
b. Gerente General
c. Líder de proceso de Aseguramiento del Servicio
d. Líder de proceso de Centro de Información y Gestión.
e. Líder del proyecto

Este comité, tuvo como finalidad establecer el nivel de cumplimiento de los requerimientos contractuales y definir las repercusiones legales que tendría la organización en su incumplimiento.

A continuación se nombran apartes del contrato en los que incurre la organización en temas relacionados con la seguridad de la información.

- Especificaciones funcionales de las aplicaciones informáticas del sistema de recaudo.

Las aplicaciones informáticas del sistema de recaudo que se instalen en el computador central, deberán cumplir las siguientes especificaciones funcionales mínimas según lo establecido en el contrato.

- Operación de la unidad de procesamiento de datos

La operación de la unidad de procesamiento de datos incluye la administración de los trabajos y monitoreo del desempeño de la máquina, administración de la seguridad, administración de la base de datos, administración de las configuraciones, la administración del ambiente de desarrollo y la administración de las cintas y la seguridad física del centro de cómputo.

- Control de acceso a la información del sistema de recaudo

El sistema de recaudo deberá tener un mecanismo para controlar el acceso de los usuarios de información a los datos del recaudo

- Integridad de la información

El Sistema debe contar con rutinas de verificación de integridad de la información. Los errores detectados deberán ser corregidos automáticamente para impedir la propagación de datos inválidos a lo largo de la base de datos. Las transacciones duplicadas o incompletas se deberán detectar y corregir sin que ello implique una detención total del Sistema. En el caso de una transacción incompleta o de interrupciones en la comunicación la parte del Sistema afectada deberá reparar y registrar inmediatamente el error.

- Encripción de la información almacenada

Los equipos del sistema de recaudo deberán disponer de llaves de encripción (encriptación) y de desencripción (desencriptación) que permitan que toda la información transmitida y almacenada en ellos esté encriptada.

En el gráfico1, se puede determinar la interacción del sistema de información de Transmilenio S.A y el enlace con Angelcom S:A.

SISTEMA OPERATIVO DE INFORMACIÓN DE ANGELCOM S.A.

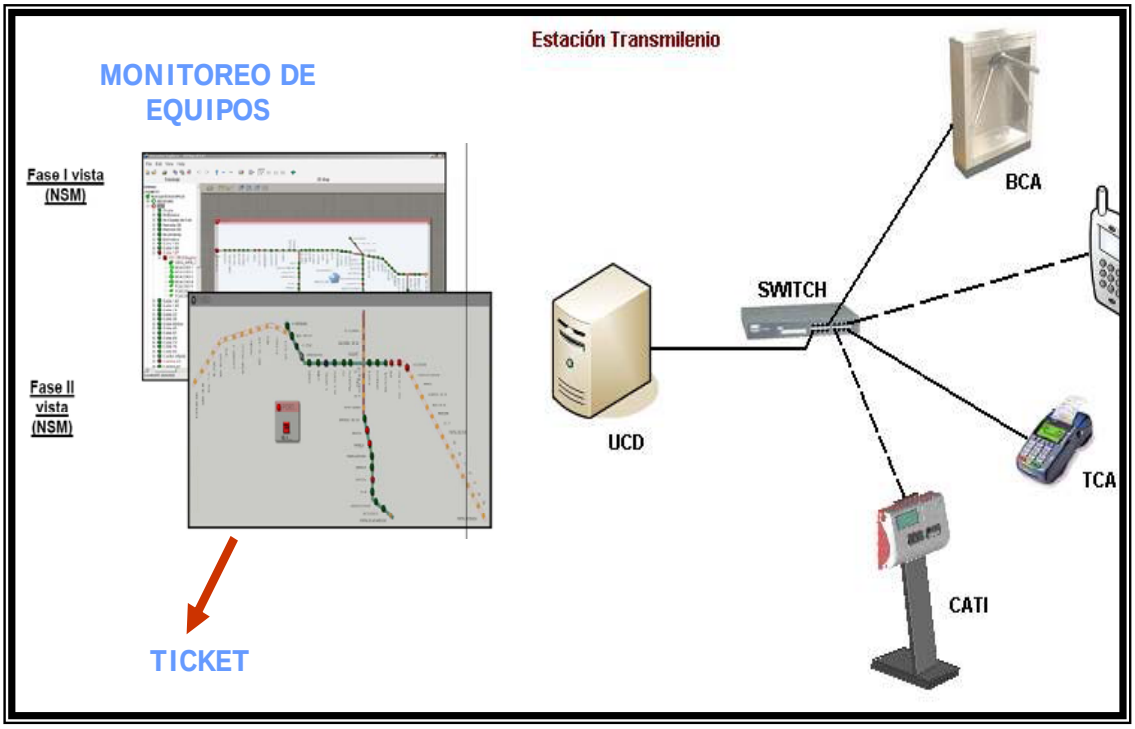

FIGURA 5

Fuente: Contrato de Concesión.

IDENTIFICACIÓN Y NIVEL DE CUMPLIMIENTO DE LOS REQUERIMIENTOS DE SEGURIDAD INFORMÁTICA DE ANGELCOM S.A

REQUERIMIENTOS CONTRACTUALES	NIVEL DE CUMPLIMIENTO			APLICACIONES	CONTROLES
	ALTO	MEDIO	BAJO		
Administración de las transacciones: almacenamiento, enrutamiento, procesamiento y autorización de todas las transacciones generadas en el sistema, venta de boletos magnéticos, venta y recarga de tarjetas inteligentes, validaciones de entrada y de salida de pasajeros en las barreras de control de acceso de los puntos de parada, mensajes de error o falla de los equipos, codificación de los boletos magnéticos e inicialización de las tarjetas inteligentes.	X			SERVICE DESK; ORACLE, SIPRA;	INDICADORES DE CONTROL "TIEMPO OPORTUNO REPORTES DE VENTA Y PASADAS"
Gestión de emisión de crédito: Autorización de codificación de los boletos magnéticos o recarga de tarjetas inteligentes. Cada codificador o vendedor deberá tener asignado un cupo de crédito autorizado por el CONCESIONARIO en el computador central.			X	SIPRA	NO HAY CONTROLES EXISTENTES: GENERAR INDICADOR DE ADMINISTRACION DE TARJETAS
Generación de reportes: El computador central debe generar los reportes de transacciones generadas por los medios de pago en el Sistema TransMilenio, tales como las frecuencias por tipo de tarifa, la matriz origen destino de pasajeros, los patrones de entrada y salida por hora, la historia de las utilizaciones de las tarjetas inteligentes, alarmas, frecuencias y localización de fallas, entre otros indicadores, y los demás reportes que le solicite TRANSMILENIO S.A. y/o que sean requeridos para el seguimiento y control del comportamiento del recaudo y de las condiciones de utilización del Sistema TransMilenio por parte de los usuarios.	X			SERVICE DESK; ORACLE, SIPRA;	MONITOREO EN VISTA DE NEGOCIOS; BASE DE DATOS Y MESA DE AYUDA
Conciliación de transacciones: El centro de computo, después de recolectar los datos de las transacciones, deberá calcular el ingreso diario total para enviarlo a TRANSMILENIO S.A. y al administrador fiduciario del Sistema TransMilenio.	X			UPD	CERTIFICACION DE DINEROS RECAUDADOS
Detección de fraude del Sistema: El sistema de recaudo deberá controlar el fraude en las tarjetas inteligentes sin contacto, verificando que las validaciones no excedan a las recargas, conciliando los boletos magnéticos validados contra los boletos magnéticos vendidos, y detectando la validación de boletos magnéticos ilegales para retenerlos inmediatamente.	X			UPD	NO HAY CONTROLES EXISTENTES: GENERAR REPLICAS DE INFORMACION; GENERAR INDICADOR ROTACION Y SEGUIMIENTO DE TISC
Listas de medios de pago no válidos para el sistema: Deberán almacenar los registros de todas las tarjetas inteligentes o boletos magnéticos reportados como perdidos o robados. Los boletos magnéticos que se encuentren registrados en las listas de medios de pago no válidos para el sistema, deberán ser almacenados por un tiempo igual o superior al tiempo de vencimiento del boleto magnético. De igual manera se procederá con las tarjetas inteligentes en el caso de encontrarse estas registradas en las listas mencionadas, caso en el cual deberán ser almacenadas por un tiempo igual o superior a tres (3) años.	X			SIPRA; UPD	INDICADOR DE LISTAS NEGRAS Y BLANCAS
Monitoreo de problemas: El computador de mantenimiento debe registrar el estado de todos los equipos del sistema de recaudo. Los equipos con problemas deben listarse en el monitor del computador de mantenimiento, para que el oficial de mantenimiento que recibe el reporte se dirija al punto de parada inmediatamente y repare el problema, en el plazo que corresponda conforme a los niveles de servicio exigidos en el presente contrato.	X			SERVICE DESK	MENSAJERIA AUTOMATICA; REPORTES DE INCIDENCIAS
Datos estadísticos de mantenimiento: Se deberá mantener un control sobre el número de transacciones de cada equipo para realizar el mantenimiento preventivo y para determinar los niveles de inventario de repuestos.	X			SERVICE DESK-SIPRA	INDICADOR REPORTE DE TRANSACCIONES
Historia de mantenimiento: El módulo de mantenimiento deberá tener información respecto de la historia de mantenimiento de cada uno de los módulos y/o equipos del sistema de recaudo, incluidos los equipos de reemplazo.		X		SERVICE DESK	MONITOREO EN VISTA DE NEGOCIOS; BASE DE DATOS Y MESA DE AYUDA
Administración de inventarios: El Sistema deberá registrar, controlar y administrar el estado y la localización de cada activo del sistema de recaudo (equipos de cómputo, las aplicaciones informáticas, muebles, partes y repuestos, entre otros).	X			SERVICE DESK	MONITOREO EN VISTA DE NEGOCIOS; BASE DE DATOS Y MESA DE AYUDA
Protección de la información: Toda la información debe protegerse de pérdida, modificación y/o divulgación desautorizada mientras se almacena o se transmite de un equipo a otro dentro del sistema de recaudo. Estos equipos deberán estar protegidos con contraseñas de acceso.		X		UPD	NO HAY CONTROLES EXISTENTES: CREAR PROCEDIMIENTO DE SINCRONIZACION DE REPLICA
Funciones administrativas: El sistema central deberá contar con las funciones para la administración de los usuarios de información del sistema de recaudo, de configuraciones y de equipos del sistema, tales como la asignación de usuarios, claves, etc			X	UPD	NO HAY CONTROLES EXISTENTES: CREAR PROCEDIMIENTO DE CREACION DE ROLES Y USUARIOS EN BASE DE DATOS

TABLA 9

Fuente: Contrato de Concesión

3. TASACIÓN DE ACTIVOS

Para la tasación de activos de información de cada uno de los procesos críticos, se utilizo la escala de Likert en donde se tomaron los siguientes valores.

ESCALA DE LIKERT

ESCALA	VALOR
MUY BAJO	1
BAJO	2
MEDIO	3
ALTO	4
MEDIO ALTO	5

TABLA 10.

Fuente: www.eumed.net/libros/introduccionalametodologiadelainformacion

La pregunta que se efectuó para hacer uso de la escala fue: ¿Cómo una pérdida o una falla en un determinado activo, afecta la confidencialidad, integridad y disponibilidad de la información?

Para la tasación de activos se convoco a una reunión con cada uno de los líderes de proceso de Aseguramiento del servicio y Centro de Información y Gestión quienes se les realizo una inducción con los siguientes temas:

- Definición de un activo de información.
- Modalidades de activos de información
- Tasación de activos de información.

Después de conceptualizar a los líderes de proceso con la información dada para la tasación de activos se realizo nuevamente un comité donde se encontraban los siguientes funcionarios:

- Gerente General
- Líder de proceso de Aseguramiento del Servicio
- Líder de proceso de Centro de Información y Gestión.
- Líder del proyecto
- Coordinador de Mejoramiento Continuo.

Bajo este esquema y de acuerdo a la escala y a los activos identificados previamente se definió cuales afectan la confidencialidad, integridad y disponibilidad de la información; obteniendo como resultados lo siguiente: Ver tabla 11

TASACIÓN DE ACTIVOS DE INFORMACIÓN DE

ASEGURAMIENTO DEL SERVICIO

			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos	2	4	5	4
		Incidencias Operativas	3	4	5	4
		Configuraciòn dispositivos de memoria	3	4	5	4
		Versiones de Firmware	5	4	5	5
		Actualización remota	4	4	5	4
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso	4	4	5	4
		Entregas de obras Transmilenio	4	3	5	4
		Contrato de concesion	4	4	5	4
		Especificaciones tecnicas de equipos	4	4	5	4
	ACTIVOS DE SOFTWARE	Windows NT	2	2	5	3
		Linux	3	2	5	3
		Favila	5	2	5	4
		Ovunto	2	2	5	3
		NSM	2	3	5	3
		Service Desk	2	3	5	3
		Intranet	4	2	5	4
		Putty	3	2	5	3
	ACTIVOS FISICOS	Equipos de configuracion	2	4	5	4
		Equipos de recaudo	4	5	5	5
		Servidores	5	5	4	5
		Banco de pruebas	4	5	5	5
	PERSONAL	Auxiliar de Mantenimiento de equipos	4	4	4	4
		Auxiliar Administrativa de activos	4	4	4	4
		Auxiliar de Mantenimiento Almacen Satelite	4	4	4	4

TABLA 11.

Fuente: norma ISO/IEC 17799:2005 y Caracterizaciones CA-MA-002

TASACIÓN DE ACTIVOS DE INFORMACIÓN DE

CENTRO DE INFORMACIÓN Y GESTIÓN

			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
CENTRO DE INFORMACION Y GESTION	ACTIVOS DE INFORMACION	Base de datos estaciones	4	5	5	5
		Base de datos transacciones	5	5	5	5
		Base de datos pasadas	5	5	5	5
		Versiones de Software	5	5	5	5
		Base de datos usuarios	4	4	4	4
		Desencole dispositivos de almacenamiento	5	5	5	5
		Protocolos IP de equipos de recaudo	5	5	5	5
		Protocolos IP de equipos de computo	5	5	5	5
		Acceso remoto	5	5	5	5
		Listas negras	5	5	5	5
		Listas blancas	5	5	5	5
	DOCUMENTOS DE PAPEL	Protocolos de software	3	4	4	4
		Bitacoras de acceso Centro de Computo	3	4	3	3
		Certificado digital	3	5	3	4
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication	5	5	5	5
		ServiceDev	5	5	5	5
		Toad	5	5	5	5
		Protocolo TCP/IP	5	5	5	5
		Batch	5	5	5	5
		VNP	5	5	5	5
		VNC	5	5	5	5
		Unicenter	5	5	5	5
	ACTIVOS FISICOS	Centro de computo	5	5	5	5
		Servidor de archivos de la organización	5	5	5	5
		Servidor base de datos	5	5	5	5
		UCD¨s (Unidad central de datos)	5	5	5	5
		Router¨s	4	5	5	5
		Switchers	4	5	5	5
		Modulos SAM Llaves de seguridad	5	5	5	5
		Servidor NSM	4	5	5	5
		Servidor SD	4	5	5	5
		Controlador de Dominio	4	5	5	5
	PERSONAL	Analista de Sistemas	4	4	4	4
		Tecnico de Sistemas	4	4	4	4
		Auxiliar de Soporte	4	4	4	4
		Administrador Base de datos	4	4	4	4
		Operario de Informatica	4	4	4	4

TABLA 12..

Fuente: norma ISO/IEC 17799:2005 y Caracterizaciones CA-MA-002

Teniendo en cuenta la tasación realizada, la organización pudo evidenciar cuales de los activos de información son de mayor impacto y se consideran importantes para la ejecución propia de la operación del sistema; por lo tanto para mayor comprensión se graficó el comportamiento de cada proceso según la confidencialidad, integridad y disponibilidad.

COMPORTAMIENTO DE CADA PROCESO SEGÚN LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

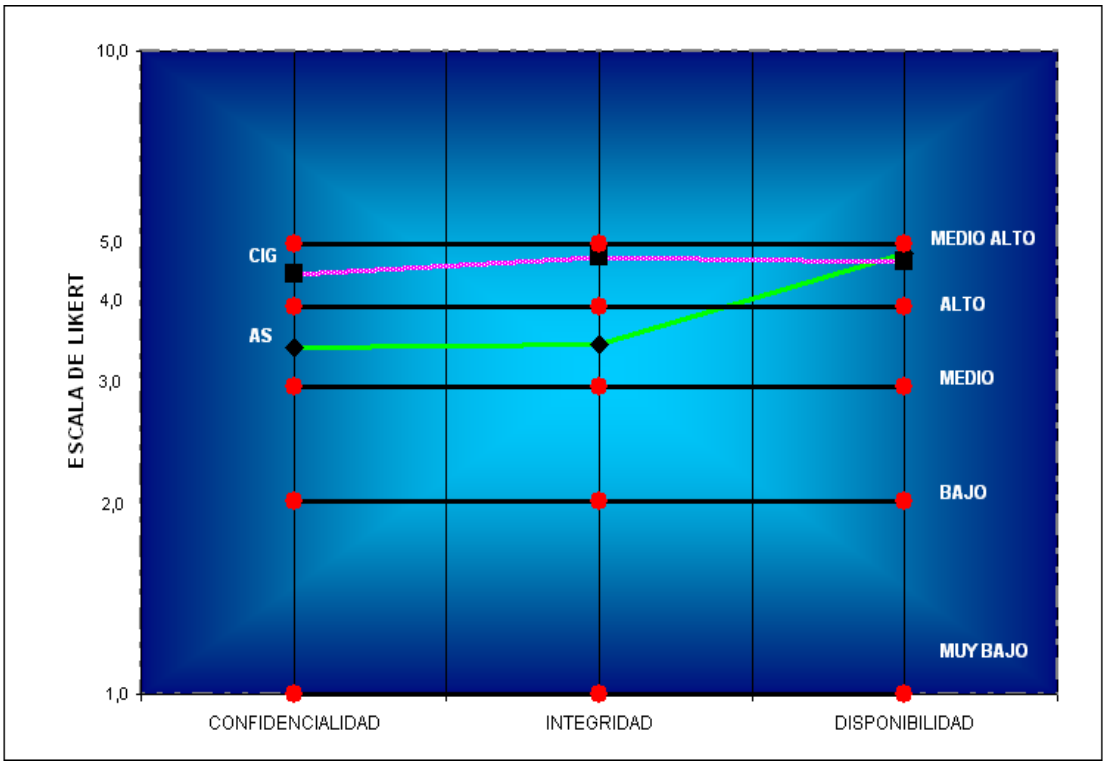

GRÁFICO 1

Fuente: Resultados de tabla 11 y tabla 12.

Del gráfico 1 se puede deducir lo siguiente:

- El proceso de Aseguramiento del Servicio cuenta con un nivel medio alto de falencias de disponibilidad de información, lo cual indica que es un proceso crítico pero no afecta la operatividad, sin embargo presenta la Confidencialidad e integridad en un nivel medio y alto, lo que representa ausencia de controles.

- El proceso de Centro de Información y Gestión se encuentra en un nivel medio alto para los tres parámetros, Confidencialidad, Integridad y

Disponibilidad lo que indica que es un proceso crítico y los riesgos asociados pueden afectar la información de la organización.

4. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En la organización; los activos de información podían estar sujetos a distintas formas de amenazas. “Un amenaza es la indicación de un potencial evento no deseado”, por el cual para que una amenaza cause daño a algún activo de información tendría que explotar una o mas vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño.

“Una amenaza es la indicación de un potencial evento no deseado” (Alberts y Dorofee, 2003). En esta definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural. En su libro Information Security Risk Analisis (Thomas Welter, 2001) plantea los diferentes clases de amenazas.

En la figura 3 se mencionan los 6 tipos de amenazas estandarizadas las cuales están bajo estudio para determinar la posibilidad de ocurrencia a partir de los activos de información ya detectados.

AMENAZAS BAJO EL MÉTODO DREAD

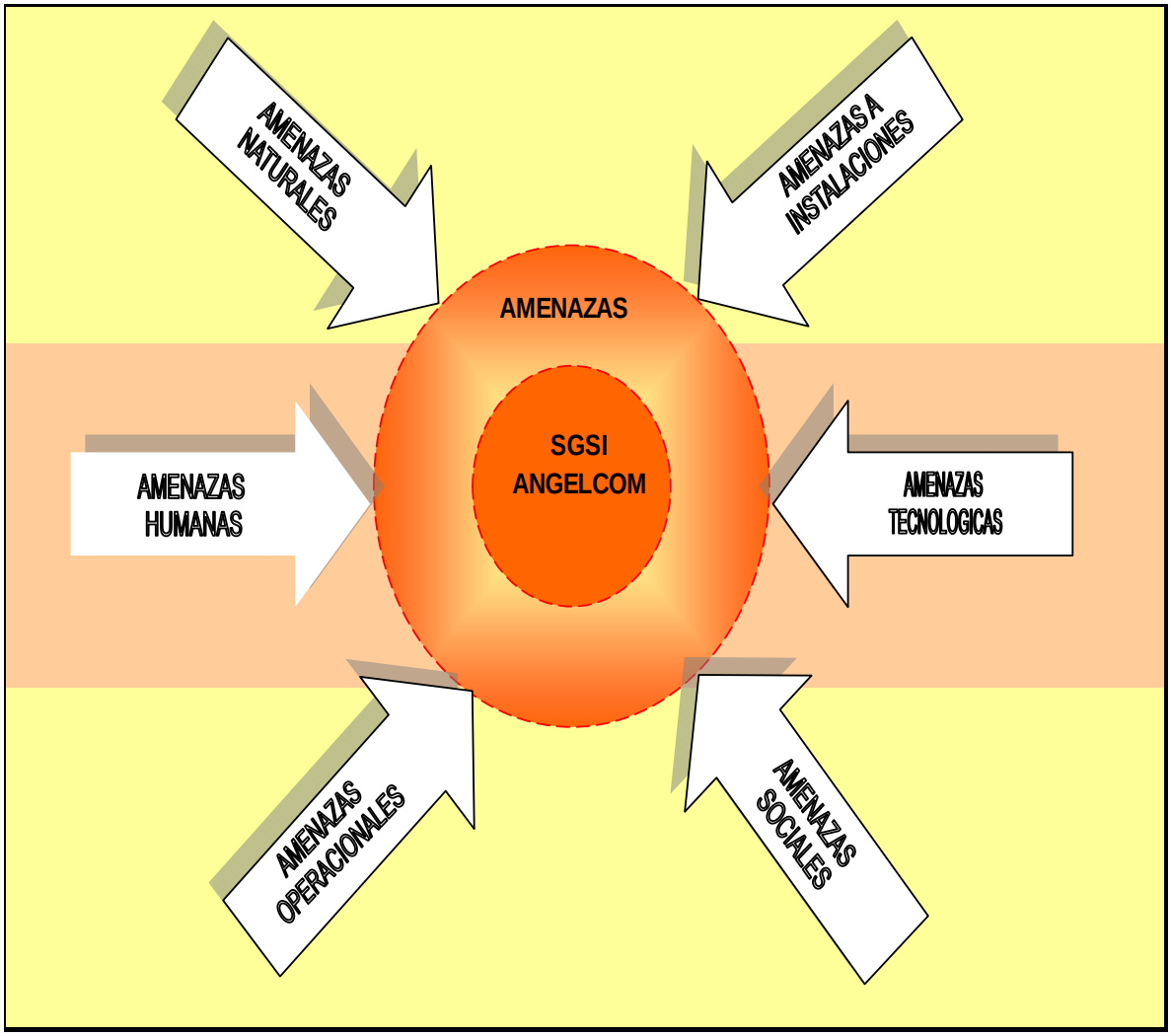

FIGURA 3.

Fuente: Thomas Welter,2001.Information Security Risk Analisis

A mediados del 2006, Microsoft anuncio lo que denomina ACE Threat Análisis and Modeling V2, una metodología para la identificación de amenazas de acuerdo a las necesidades de la organización.

Bajo esta metodología se crea el método **DREAD**, que trata de facilitar el uso de un criterio común respondiendo a las siguientes cuestiones y de esta manera comprender cuales son las amenazas que afectan el sistema

- **Damage potential** (Daño potencial): ¿Cual es el daño que puede originar la vulnerabilidad si llega a ser explotada?

- **Reproducibility** (Reproducibilidad): ¿Es fácil reproducir las condiciones que propicien el ataque?

- **Exploitability** (Explotabilidad): ¿Es sencillo llevar a cabo el ataque?

- **Affected users** (Usuarios afectados): ¿Cuantos usuarios se verían afectados?

- **Discoverability** (Descubrimiento): ¿Es fácil encontrar la vulnerabilidad?

A continuación se muestra una tabla para priorizar las amenazas de acuerdo a los activos de información identificados por cada proceso y los tipos de amenazas como se muestra en la figura 3.

METODOLOGÍA PARA PRIORIZAR LAS AMENAZAS

PUNTUACION	ALTO	MEDIO	BAJO
DAÑO POTENCIAL	El atacante podría ejecutar aplicaciones con permiso de administrador; subir contenido.	Divulgación de información sensible	Divulgación de información trivial
REPRODUCIBILIDAD	El ataque es fácilmente reproducible.	El ataque se podría reproducir, pero sólo en condiciones muy concretas, ejemplo: condición de carrera.	Ataque difícil de reproducir, incluso conociendo la naturaleza del fallo.
EXPLOTABILIDAD	Un programador novel podría implementar el ataque en poco tiempo.	Un programador experimentado podría implementar el ataque.	Se requieren ciertas habilidades y conocimientos para explotar la vulnerabilidad.
USUARIOS AFECTADOS	Todos los usuarios, configuración por defecto ...	Algunos usuarios, no es la configuración por defecto.	Pocos usuarios afectados.
DESCUBRIMIENTO	Existe información pública que explica el ataque. Vulnerabilidad presente en una parte de la aplicación muy utilizada.	La vulnerabilidad afecta a una parte de la aplicación que casi no se utiliza. No es muy probable que sea descubierta.	El fallo no es trivial, no es muy probable que los usuarios puedan utilizarlo para causar un daño potencial.

TABLA 13

Fuente: ACE Threat Análisis and Modeling V2

ESCALA	VALOR
MUY BAJO	1
BAJO	2
MEDIO	3
ALTO	4
MEDIO ALTO	5

Escala de Likert Fuente: www.eumed.net/libros/introduccionalametodologiadelainformacion

Según el ACE Team, el defensor está en una posición mejor que el atacante para comprender cuales son las amenazas que afectan al sistema. Se presupone que las distintas personas implicadas en su desarrollo y puesta en funcionamiento conocen de manera directa que es lo que hace el software, cómo lo hace y cuales serian las partes más vulnerables. Mientras que un atacante debe orientarse únicamente haciendo uso de especulaciones en base a su observación y las pruebas que efectúa sobre las partes de la aplicación expuestas públicamente o que han sido descubiertas durante la etapa de reconocimiento en un ataque.

Una vez identificadas las amenazas; se comenzó a analizar que tipos de amenazas podían afectar la confidencialidad, integridad y disponibilidad de la información de la organización, obteniendo los siguientes resultados:

CLASIFICACIÓN DE LAS AMENAZAS

AMENAZAS NATURALES	INUNDACIONES
	SISMOS
	TORMENTAS
AMENAZAS A INSTALACIONES	FUEGO
	EXPLOSION
	CAIDA DE ENERGIA
	PERDIDA DE ACCESO
	DAÑO EN PLANTA ELECTRICA
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE
	PROBLEMAS DE TRANSPORTE
AMENAZAS TECNOLOGICAS	VIRUS
	PERDIDA DE DATOS
	FALLAS DE HARDWARE
	FALLAS DE SOFTWARE
	FALLAS DE RED
	FALLAS EN LINEAS TELEFONICAS
	FALLAS EN ANTENAS DE COMUNICACIÓN
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO
	FALLAS EN LAS REPLICAS DE TRANSMILENIO
AMENAZAS SOCIALES	MOTINES
	PROTESTAS
	BOMBAS
	TERRORISMO

TABLA 14

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

Con lo anterior; se determinaron bajo la escala de likert que activos de la información de los procesos críticos afectan la información; lo cual tanto para el proceso de Aseguramiento del Servicio como para el proceso de Centro de Información y Gestión la probabilidad de ocurrencia de amenazas se encontraban en un nivel bajo; lo que indica que la organización debe tomar decisiones importantes en relación con el análisis de las amenazas. La decisión sobre cuáles amenazas se descarta, por tener éstas una ocurrencia baja; depende de las consecuencias económicas que pudiera incurrir la organización. A continuación se relaciona por proceso la probabilidad de amenaza según los activos de información identificados.

Para la recolección de la información de la priorización de amenazas, se generó un comité donde se evaluaba según el método expuesto la priorización de amenazas según proceso. Para este comité se convoco a los siguientes funcionarios:

- Gerente General
- Líder de proceso de Aseguramiento del Servicio
- Líder de proceso de Centro de Información y gestión
- Líder de proyecto
- Coordinador Mejoramiento Continuo.

AMENAZAS DE ASEGURAMIENTO DEL SERVICIO (AMENAZA NATURAL, AMENAZAS A INSTALACIONES)

			AMENAZA NATURAL			AMENAZAS A INSTALACIONES			
			INUNDACIONES	SISMOS	TORMENTAS	FUEGO	EXPLOSION	CAIDA DE ENERGIA	PERDIDA DE ACCESO
ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos	1	1	4	2	3	5	4
		Incidencias Operativas	1	1	1	1	2	5	4
		Configuraciòn dispositivos de memoria	1	1	4	1	1	2	1
		Versiones de Firmware	1	1	4	1	1	1	1
		Actualización remota	1	1	4	1	1	1	1
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso	1	1	1	1	1	1	1
		Entregas de obras Transmilenio	1	1	1	1	1	1	1
		Contrato de concesion	1	1	1	1	1	1	1
		Especificaciones tecnicas de equipos	1	1	1	1	1	1	1
	ACTIVOS DE SOFTWARE	Windows NT	1	1	2	1	1	3	4
		Linux	1	1	2	1	1	3	4
		Faxila	1	1	2	1	1	3	4
		Ovunto	1	1	b	1	1	3	4
		NSM	1	1	2	1	1	3	4
		Service Desk	1	1	2	1	1	3	4
		Intranet	1	1	2	1	1	3	4
		Putty	1	1	2	1	1	3	4
	ACTIVOS FISICOS	Equipos de configuracion	1	1	2	1	1	3	2
		Equipos de recaudo	1	1	4	1	1	4	3
		Servidores	1	1	4	1	1	4	3
		Banco de pruebas	1	1	2	1	1	1	1
	PERSONAL	Auxiliar de Mantenimiento de equipos	1	1	1	1	1	1	1
		Auxiliar Administrativa de activos	1	1	1	1	1	1	1
		Auxiliar de Mantenimiento Almacen Satelite	1	1	1	1	1	1	1
	TOTALES:		1	1	2	1	1	2	2

TABLA 15.

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

AMENAZAS DE ASEGURAMIENTO DEL SERVICIO (AMENAZAS HUMANAS, AMENAZAS TECNOLOGICAS)

			AMENAZAS HUMANAS		AMENAZAS TECNOLOGICAS						
			PERDIDA DE PERSONAL CLAVE	PROBLEMAS DE TRANSPORTE	VIRUS	PERDIDA DE DATOS	FALLAS DE HARDWARE	FALLAS DE SOFTWARE	FALLAS DE RED	FALLAS EN LINEAS TELEFONICAS	FALLAS EN ANTENAS DE COMUNICACIÓN
ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos	1	1	1	3	5	5	5	3	3
		Incidencias Operativas	1	1	1	4	4	4	3	1	1
		Configuraciòn dispositivos de memoria	3	1	1	1	4	4	4	1	1
		Versiones de Firmware	1	1	1	1	4	4	4	1	1
		Actualización remota	3	1	1	4	4	4	3	1	1
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso	1	1	1	1	1	1	2	1	1
		Entregas de obras Transmilenio	1	1	1	1	1	1	1	1	1
		Contrato de concesion	1	1	1	1	1	1	1	1	1
		Especificaciones tecnicas de equipos	1	1	1	1	1	1	1	1	1
	ACTIVOS DE SOFTWARE	Windows NT	1	1	3	4	4	2	4	1	1
		Linux	3	1	1	1	4	3	3	1	1
		Faxila	3	1	1	1	4	3	3	1	1
		Ovunto	3	1	1	1	4	3	3	1	1
		NSM	1	1	1	3	4	3	3	1	1
		Service Desk	1	1	1	4	4	3	4	1	1
		Intranet	1	1	4	4	4	3	4	1	1
		Putty	1	1	1	1	4	3	4	1	1
	ACTIVOS FISICOS	Equipos de configuracion	1	1	1	1	4	1	1	1	1
		Equipos de recaudo	1	1	1	4	5	5	1	1	5
		Servidores	1	1	1	4	5	5	2	1	3
		Banco de pruebas	1	1	1	1	4	1	1	1	1
	PERSONAL	Auxiliar de Mantenimiento de equipos	3	3		1	1	1	1	1	1
		Auxiliar Administrativa de activos	2	1		1	1	1	1	1	1
		Auxiliar de Mantenimiento Almacen Satelite	3	3		1	1	1	1	1	1
	TOTALES:		2	1	1	2	3	3	3	1	1

TABLA 16.

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

AMENAZAS DE ASEGURAMIENTO DEL SERVICIO (AMENAZAS OPERACIONALES, AMENAZAS SOCIALES

			AMENAZAS OPERACIONALES		AMENAZAS SOCIALES			
			FALLAS EN CCR	FALLAS EN LAS REPLICAS DE TRANSMILENIO	MOTINES	PROTESTAS	BOMBAS	TERRORISMO
ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos	3	4	1	1	3	3
		Incidencias Operativas	1	4	1	1	3	3
		Configuraciòn dispositivos de memoria	1	1	1	1	3	3
		Versiones de Firmware	1	1	1	1	1	1
		Actualización remota	1	1	1	1	1	1
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso	1	1	1	1	1	1
		Entregas de obras Transmilenio	1	1	1	1	1	1
		Contrato de concesion	1	1	1	1	1	1
		Especificaciones tecnicas de equipos	1	1	1	1	1	1
	ACTIVOS DE SOFTWARE	Windows NT	1	1	1	1	1	1
		Linux	1	1	1	1	1	1
		Faxila	1	1	1	1	1	1
		Ovunto	1	1	1	1	1	1
		NSM	1	1	1	1	1	1
		Service Desk	1	1	1	1	1	1
		Intranet	1	1	1	1	1	1
		Putty	1	1	1	1	1	1
	ACTIVOS FISICOS	Equipos de configuracion	1	1	1	1	1	1
		Equipos de recaudo	1	1	1	1	4	4
		Servidores	1	1	1	1	1	1
		Banco de pruebas	1	1	1	1	1	1
	PERSONAL	Auxiliar de Mantenimiento de equipos	1	1	1	1	1	1
		Auxiliar Administrativa de activos	1	1	1	1	1	1
		Auxiliar de Mantenimiento Almacen Satelite	1	1	1	1	1	1
	TOTALES:		1	1	1	1	1	1

TABLA 17

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

AMENAZAS DE CENTRO DE INFORMACIÓN Y GESTIÓN (AMENAZA NATURAL, AMENAZAS A INSTALACIONES)

			AMENAZA NATURAL			AMENAZAS A INSTALACIONES				
			INUNDACIONES	SISMOS	TORMENTAS	FUEGO	EXPLOSION	CAIDA DE ENERGIA	PERDIDA DE ACCESO	DAÑO EN PLANTA ELECTRICA
CENTRO DE INFORMACION Y GESTION	ACTIVOS DE INFORMACION	Base de datos estaciones	1	1	1	1	1	3	3	4
		Base de datos transacciones	1	1	1	1	1	3	4	4
		Base de datos pasadas	1	1	1	1	1	3	4	4
		Versiones de Software	1	1	1	1	1	3	4	4
		Base de datos usuarios	1	1	1	1	1	3	4	4
		Desencole dispositivos de almacenamiento	1	1	1	1	1	3	5	4
		Protocolos IP de equipos de recaudo	1	1	1	1	1	3	5	4
		Protocolos IP de equipos de computo	1	1	1	1	1	3	3	4
		Acceso remoto	1	1	1	1	1	3	2	4
		Listas negras	1	1	1	1	1	3	4	4
		Listas blancas	1	1	1	1	1	3	4	4
	DOCUMENTOS DE PAPEL	Protocolos de software	1	1	1	1	1	1	1	1
		Bitacoras de acceso Centro de Computo	1	1	1	1	1	1	1	1
		Certificado digital	1	1	1	1	1	1	1	1
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication	1	1	1	1	1	3	4	4
		ServiceDev	1	1	1	1	1	3	4	4
		Toad	1	1	1	1	1	3	4	4
		Protocolo TCP/IP	1	1	1	1	1	3	4	4
		Batch	1	1	1	1	1	3	4	4
		VNP	1	1	1	1	1	3	4	4
		VNC	1	1	1	1	1	3	4	4
		Unicenter	1	1	1	1	1	3	4	4
	ACTIVOS FISICOS	Centro de computo	1	1	3	4	1	5	1	5
		Servidor de archivos de la organización	1	1	1	1	1	5	2	5
		Servidor base de datos	1	1	1	1	1	5	2	5
		UCD¨s (Unidad central de datos)	1	1	1	1	1	5	2	5
		Router¨s	1	1	1	4	1	5	1	5
		Switchers	1	1	1	1	1	5	1	5
		Modulos SAM Llaves de seguridad	1	1	1	1	1	1	1	1
		Servidor NSM	1	1	1	1	1	5	1	5
		Servidor SD	1	1	1	1	1	5	1	5
		Controlador de Dominio	1	1	1	1	1	1	1	5
	PERSONAL	Analista de Sistemas	2	2	2	1	1	1	1	1
		Tecnico de Sistemas	2	2	2	1	1	1	1	1
		Auxiliar de Soporte	2	2	2	1	1	1	1	1
		Administrador Base de datos	2	2	2	1	1	1	1	1
		Operario de Informatica	2	2	2	1	1	1	1	1
			1	**1**	**1**	**1**	**1**	**3**	**3**	**4**

TABLA 18

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

AMENAZAS DE CENTRO DE INFORMACIÓN Y GESTIÓN (AMENAZAS HUMANAS, AMENAZAS TECNOLOGICAS)

			AMENAZAS HUMANAS		AMENAZAS TECNOLOGICAS						
			PERDIDA DE PERSONAL CLAVE	PROBLEMAS DE TRANSPORTE	VIRUS	PERDIDA DE DATOS	FALLAS DE HARDWARE	FALLAS DE SOFTWARE	FALLAS DE RED	FALLAS EN LINEAS TELEFONICAS	FALLAS EN ANTENAS DE COMUNICACIÓN
CENTRO DE INFORMACION Y GESTION	ACTIVOS DE INFORMACION	Base de datos estaciones	1	1	1	2	2	3	1	1	3
		Base de datos transacciones	1	1	1	5	4	3	1	1	3
		Base de datos pasadas	1	1	1	5	4	3	1	1	3
		Versiones de Software	2	1	1	1	4	4	1	1	3
		Base de datos usuarios	1	1	1	1	1	1	1	1	3
		Desencole dispositivos de almacenamiento	2	1	1	5	5	4	1	1	1
		Protocolos IP de equipos de recaudo	3	1	1	5	5	4	4	1	3
		Protocolos IP de equipos de computo	3	1	1	4	1	2	4	1	1
		Acceso remoto	1	1	1	1	1	2	1	1	1
		Listas negras	1	1	1	4	4	4	1	1	1
		Listas blancas	1	1	1	4	4	4	1	1	1
	DOCUMENTOS DE PAPEL	Protocolos de software	1	1	1	2	1	1	1	1	1
		Bitacoras de acceso Centro de Computo	1	1	1	1	1	1	1	1	1
		Certificado digital	1	1	1	1	1	1	1	1	1
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication	1	1	2	4	4	4	4	3	1
		ServiceDev	1	1	1	4	4	4	3	1	1
		Toad	1	1	1	4	4	4	3	1	1
		Protocolo TCP/IP	1	1	1	4	4	4	3	1	3
		Batch	1	1	1	4	4	4	3	1	1
		VNP	1	1	2	4	4	4	4	1	1
		VNC	1	1	2	4	4	4	4	1	1
		Unicenter	1	1	1	4	4	4	3	1	1
	ACTIVOS FISICOS	Centro de computo	1	1	4	5	5	5	4	1	4
		Servidor de archivos de la organización	1	1	4	5	5	5	4	1	1
		Servidor base de datos	1	1	4	5	5	5	4	1	1
		UCD¨s (Unidad central de datos)	2	1	4	5	5	5	4	1	1
		Router¨s	3	1	1	1	5	5	3	1	1
		Switchers	3	1	1	1	5	5	3	1	4
		Modulos SAM Llaves de seguridad	1	1	1	1	5	1	1	1	1
		Servidor NSM	1	1	4	4	5	5	3	1	1
		Servidor SD	1	1	4	4	5	5	3	1	1
		Controlador de Dominio	1	1	4	4	5	5	1	1	1
	PERSONAL	Analista de Sistemas	4	2	1	1	1	1	1	1	1
		Tecnico de Sistemas	3	2	1	1	1	1	1	1	1
		Auxiliar de Soporte	3	2	1	1	1	1	1	1	1
		Administrador Base de datos	4	2	1	1	1	1	1	1	1
		Operario de Informatica	2	2	1	1	1	1	1	1	1
			2	1	2	3	3	3	2	1	2

TABLA 19

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

AMENAZAS DE CENTRO DE INFORMACIÓN Y GESTIÓN (AMENAZAS OPERACIONALES, AMENAZAS SOCIALES

			AMENAZAS OPERACIONALES		AMENAZAS SOCIALES			
			FALLAS EN CCR	FALLAS EN LAS REPLICAS DE TRANSMILENIO	MOTINES	PROTESTAS	BOMBAS	TERRORISMO
CENTRO DE INFORMACION Y GESTION	ACTIVOS DE INFORMACION	Base de datos estaciones	4	4	1	1	2	2
		Base de datos transacciones	4	4	1	1	2	2
		Base de datos pasadas	4	4	1	1	2	2
		Versiones de Software	4	4	1	1	2	2
		Base de datos usuarios	4	1	1	1	2	2
		Desencole dispositivos de almacenamiento	4	1	1	1	2	2
		Protocolos IP de equipos de recaudo	4	1	1	1	2	2
		Protocolos IP de equipos de computo	4	1	1	1	2	2
		Acceso remoto	4	1	1	1	2	2
		Listas negras	4	1	1	1	2	2
		Listas blancas	4	1	1	1	2	2
	DOCUMENTOS DE PAPEL	Protocolos de software	1	1	1	1	2	2
		Bitacoras de acceso Centro de Computo	1	1	1	1	2	2
		Certificado digital	1	1	1	1	2	2
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication	4	4	1	1	2	2
		ServiceDev	1	1	1	1	2	2
		Toad	1	1	1	1	2	2
		Protocolo TCP/IP	1	1	1	1	2	2
		Batch	1	1	1	1	2	2
		VNP	1	1	1	1	2	2
		VNC	1	1	1	1	2	2
		Unicenter	4	4	1	1	2	2
	ACTIVOS FISICOS	Centro de computo	4	5	1	1	2	2
		Servidor de archivos de la organización	1	1	1	1	2	2
		Servidor base de datos	1	1	1	1	2	2
		UCD¨s (Unidad central de datos)	4	1	1	1	2	2
		Router¨s	1	1	1	1	2	2
		Switchers	1	1	1	1	2	2
		Modulos SAM Llaves de seguridad	1	1	1	1	2	2
		Servidor NSM	1	1	1	1	2	2
		Servidor SD	1	1	1	1	2	2
		Controlador de Dominio	1	1	1	1	2	2
	PERSONAL	Analista de Sistemas	1	1	1	1	1	1
		Tecnico de Sistemas	1	1	1	1	1	1
		Auxiliar de Soporte	1	1	1	1	1	1
		Administrador Base de datos	1	1	1	1	1	1
		Operario de Informatica	1	1	1	1	1	1
			2	2	1	1	2	2

TABLA 20

Fuente: Thomas Welter, 2001.Information Security Risk Analisis y Contrato de Concesión.

Por consiguiente, es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón era necesario entender la relación entre amenazas y vulnerabilidades. La pregunta fundamental es ¿Qué amenazas pudiesen explotar cuál de las vulnerabilidades?.

Por lo tanto las amenazas que pudiese explotar una vulnerabilidad, se muestra en la tabla 19; la cual nos permite evidenciar con claridad el impacto de cada una.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de relación de causalidad y probabilidad de ocurrencia.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo. Se han utilizado algunos apartes de la norma ISO 17799:2005 para efectuar la categorización. La clasificación fue de gran ayuda para el Diseño del Sistema de Gestión de Seguridad de la Información.

5. CÁLCULO DE LAS AMENAZAS Y VULNERABILIDADES

Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que pueden juntarse y causar un riesgo. El riesgo se define como la probabilidad de que una amenaza puede explotar una vulnerabilidad en particular (Peltier,2001).

Todo este proceso incluye calcular la posibilidad de la ocurrencia de amenazas y que tan fácil pueden ser explotadas las vulnerabilidades por las amenazas.

Para calcular la posibilidad de la presencia de amenazas, se considero los siguientes aspectos evaluados según las escala de Likert.

- **Amenazas deliberadas**: La posibilidad de amenaza deliberada en la motivación; conocimiento, capacidad y recursos disponibles para posibles atacantes.
- **Amenazas accidentales**: La posibilidad de amenaza accidental bajo la estimación de estadísticas y experiencia.
- **Incidentes del pasado**. Los incidentes ocurridos en el pasado ilustran los problemas en el actual sistema.
- **Nuevos desarrollos y sistemas**: Esto incluye novedades y tendencias de Internet.

CALCULO DE AMENAZAS V/S VULNERABILIDADES PARA LOS PROCESOS CRÍTICOS. "ASEGURAMIENTO DEL SERVICIO Y CENTRO DE INFORMACIÓN Y GESTIÓN."

VULNERABILIDADES	SEGURIDAD DE LOS RECURSOS HUMANOS				
AMENAZAS	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
AMENAZAS NATURALES	10	0	2	0	0
AMENAZAS A INSTALACIONES	11	2	4	3	0
AMENAZAS HUMANAS	5	1	1	1	0
AMENAZAS TECNOLOGICAS	6	6	1	15	0
AMENAZAS OPERACIONALES	3	1	0	4	0
AMENAZAS SOCIALES	13	1	2	0	0
	SEGURIDAD LOGICA				
	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
AMENAZAS NATURALES	15	0	0	0	0
AMENAZAS A INSTALACIONES	20	3	1	1	0
AMENAZAS HUMANAS	8	0	0	2	0
AMENAZAS TECNOLOGICAS	9	4	0	22	0
AMENAZAS OPERACIONALES	5	0	0	5	0
AMENAZAS SOCIALES	14	0	4	2	0
	SEGURIDAD FISICA Y AMBIENTAL				
	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
AMENAZAS NATURALES	15	0	0	0	0
AMENAZAS A INSTALACIONES	15	4	2	4	0
AMENAZAS HUMANAS	9	0	0	1	0
AMENAZAS TECNOLOGICAS	24	4	0	3	4
AMENAZAS OPERACIONALES	6	0	0	1	3
AMENAZAS SOCIALES	13	4	1	2	0
	GESTION DE OPERACIONES Y COMUNICACIÓN				
	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
AMENAZAS NATURALES	12	0	0	0	0
AMENAZAS A INSTALACIONES	13	5	2	0	0
AMENAZAS HUMANAS	8	0	0	0	0
AMENAZAS TECNOLOGICAS	7	7	12	2	0
AMENAZAS OPERACIONALES	6	0	0	2	0
AMENAZAS SOCIALES	15	0	0	0	0
	MANTENIMIENTO,DESARROLLO Y ADQUISICION DE SISTEMAS DE INFORMACION				
	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
AMENAZAS NATURALES	9	0	0	0	0
AMENAZAS A INSTALACIONES	14	0	0	1	0
AMENAZAS HUMANAS	6	0	0	0	0
AMENAZAS TECNOLOGICAS	7	1	5	8	0
AMENAZAS OPERACIONALES	0	0	3	3	0
AMENAZAS SOCIALES	12	0	0	0	0

TABLA 21

Fuente: norma ISO/IEC 17799:2005

La mayor parte de las intrusiones a los sistemas de información que se producen hoy en día se deben a la explotación de vulnerabilidades, por eso es de vital importancia hacer identificado aquellas vulnerabilidades susceptibles de ser aprovechadas por una amenaza, para evitar que éstas llegue a materializarse

CLASIFICACIÓN DE AMENAZA V/S CLASIFICACIÓN POR VULNERABILIDAD

"SEGURIDAD DE LOS RECURSOS HUMANOS"

		VULNERABILIDADES			
		SEGURIDAD DE LOS RECURSOS HUMANOS			
AMENAZAS		FALTA DE ENTRENAMIENTO	FALTA DE MECANISMO DE MONITOREO	FALTA DE POLITICAS	CARENCIA DE PROCEDIMIENTOS
AMENAZAS NATURALES	INUNDACIONES	1	1	1	1
	SISMOS	1	1	1	1
	TORMENTAS	3	1	1	3
AMENAZAS A INSTALACIONES	FUEGO	1	1	1	1
	EXPLOSION	1	1	1	1
	CAIDA DE ENERGIA	3	3	1	2
	PERDIDA DE ACCESO	4	2	1	1
	DAÑO EN PLANTA ELECTRICA	4	4	3	3
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE	4	1	3	2
	PROBLEMAS DE TRANSPORTE	1	1	1	1
AMENAZAS TECNOLOGICAS	VIRUS	1	3	4	4
	PERDIDA DE DATOS	1	4	4	4
	FALLAS DE HARDWARE	2	4	4	4
	FALLAS DE SOFTWARE	2	4	4	4
	FALLAS DE RED	2	4	1	4
	FALLAS EN LINEAS TELEFONICAS	2	1	1	4
	FALLAS EN ANTENAS DE COMUNICACIÓN	2	2	1	4
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO	4	4	4	4
	FALLAS EN LAS REPLICAS DE TRANSMILENIO	1	1	2	1
AMENAZAS SOCIALES	MOTINES	1	1	1	1
	PROTESTAS	1	1	1	2
	BOMBAS	1	1	1	3
	TERRORISMO	1	1	1	3

TABLA 22

Fuente: norma ISO/IEC 17799:2005

CLASIFICACIÓN DE AMENAZA V/S CLASIFICACIÓN POR VULNERABILIDAD

“SEGURIDAD LÓGICA”

		VULNERABILIDADES				
		SEGURIDAD LOGICA				
AMENAZAS		FALTA DE CONTROL DE ACCESO A LA INFORMACION	FALTA DE IDENTIFICACION Y AUTENTICACION	DEFICIENCIA EN LA MODALIDAD DE ACCESO	FALTA DE ADMINISTRACION DE PERSONAL Y USUARIOS	AUNSENCIA DE ROLES
AMENAZAS NATURALES	INUNDACIONES	1	1	1	1	1
	SISMOS	1	1	1	1	1
	TORMENTAS	1	1	1	1	1
AMENAZAS A INSTALACIONES	FUEGO	1	1	1	1	1
	EXPLOSION	1	1	1	1	1
	CAIDA DE ENERGIA	1	1	1	1	1
	PERDIDA DE ACCESO	3	2	2	2	1
	DAÑO EN PLANTA ELECTRICA	1	1	1	1	4
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE	1	1	1	4	4
	PROBLEMAS DE TRANSPORTE	1	1	1	1	1
AMENAZAS TECNOLOGICAS	VIRUS	1	4	4	4	4
	PERDIDA DE DATOS	2	4	4	4	4
	FALLAS DE HARDWARE	4	4	4	4	4
	FALLAS DE SOFTWARE	4	4	4	4	4
	FALLAS DE RED	4	4	2	4	4
	FALLAS EN LINEAS TELEFONICAS	1	1	1	1	2
	FALLAS EN ANTENAS DE COMUNICACIÓN	1	1	1	1	2
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO	4	4	4	4	4
	FALLAS EN LAS REPLICAS DE TRANSMILENIO	1	1	1	1	1
AMENAZAS SOCIALES	MOTINES	1	1	1	3	1
	PROTESTAS	1	1	1	3	1
	BOMBAS	1	1	4	1	3
	TERRORISMO	1	1	4	1	3

TABLA 23

Fuente: norma ISO/IEC 17799:2005

CLASIFICACIÓN DE AMENAZA V/S CLASIFICACIÓN POR VULNERABILIDAD

“SEGURIDAD FÍSICA Y AMBIENTAL”

		VULNERABILIDADES				
		SEGURIDAD FISICA Y AMBIENTAL				
AMENAZAS		CONTROL DE ACCESO FISICO INADECUADO	CARENCIA DE PROGRAMAS PARA SUSTITUIR EQUIPOS	DEFICIENCIA EN LA INSTALACION DE CABLEADO ESTRUCTURADO OVERHALL	ACCIONES OSTILES (ROBO, FRAUDE, SABOTAJE)	SUCEPTIBILIDAD DE EQUIPOS A VARIACIONES DE VOLTAJE
AMENAZAS NATURALES	INUNDACIONES	1	1	1	1	1
	SISMOS	1	1	1	1	1
	TORMENTAS	1	1	1	1	1
AMENAZAS A INSTALACIONES	FUEGO	3	1	2	1	1
	EXPLOSION	1	1	2	1	2
	CAIDA DE ENERGIA	4	1	2	1	4
	PERDIDA DE ACCESO	4	1	1	1	1
	DAÑO EN PLANTA ELECTRICA	1	1	3	1	4
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE	1	1	1	4	1
	PROBLEMAS DE TRANSPORTE	1	1	1	1	1
AMENAZAS TECNOLOGICAS	VIRUS	1	2	1	2	1
	PERDIDA DE DATOS	1	1	4	5	2
	FALLAS DE HARDWARE	1	1	5	5	4
	FALLAS DE SOFTWARE	1	1	4	5	2
	FALLAS DE RED	1	1	1	1	1
	FALLAS EN LINEAS TELEFONICAS	1	1	1	1	1
	FALLAS EN ANTENAS DE COMUNICACIÓN	1	1	1	1	1
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO	5	1	5	5	4
	FALLAS EN LAS REPLICAS DE TRANSMILENIO	1	1	1	1	1
AMENAZAS SOCIALES	MOTINES	1	1	1	2	1
	PROTESTAS	3	1	1	2	1
	BOMBAS	4	1	1	2	1
	TERRORISMO	4	1	1	2	1

TABLA 24

Fuente: norma ISO/IEC 17799:2005

CLASIFICACIÓN DE AMENAZA V/S CLASIFICACIÓN POR VULNERABILIDAD

"GESTIÓN DE OPERACIONES Y COMUNICACIÓN"

		VULNERABILIDADES			
		GESTION DE OPERACIONES Y COMUNICACIÓN			
AMENAZAS		COMPLICACION DE INTERFASES	GESTION DE RED INADECUADA	CARENCIA DE CONTROL DE COPIADO	FALTA DE PROTECCION DE REDES
AMENAZAS NATURALES	INUNDACIONES	1	1	1	1
	SISMOS	1	1	1	1
	TORMENTAS	1	1	1	1
AMENAZAS A INSTALACIONES	FUEGO	1	1	1	2
	EXPLOSION	1	1	1	1
	CAIDA DE ENERGIA	1	2	2	3
	PERDIDA DE ACCESO	1	2	2	3
	DAÑO EN PLANTA ELECTRICA	1	1	1	1
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE	1	1	1	1
	PROBLEMAS DE TRANSPORTE	1	1	1	1
AMENAZAS TECNOLOGICAS	VIRUS	2	4	1	1
	PERDIDA DE DATOS	3	3	4	2
	FALLAS DE HARDWARE	3	3	1	2
	FALLAS DE SOFTWARE	3	3	1	2
	FALLAS DE RED	3	3	1	2
	FALLAS EN LINEAS TELEFONICAS	3	3	1	2
	FALLAS EN ANTENAS DE COMUNICACIÓN	3	3	1	2
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO	4	4	1	1
	FALLAS EN LAS REPLICAS DE TRANSMILENIO	1	1	1	1
AMENAZAS SOCIALES	MOTINES	1	1	1	1
	PROTESTAS	11	1	1	1
	BOMBAS	1	1	1	1
	TERRORISMO	1	1	1	1

TABLA 25

Fuente: norma ISO/IEC 17799:2005

CLASIFICACIÓN DE AMENAZA V/S CLASIFICACIÓN POR VULNERABILIDAD

“MANTENIMIENTO, DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN”

		VULNERABILIDADES		
		MANTENIMIENTO,DESARROLLO Y ADQUISICION DE SISTEMAS DE INFORMACION		
AMENAZAS		CARENCIA DE VALIDACION DE DATOS	PROPAGACION DE DATOS INVALIDOS	TRANSMISION DE DATOS
AMENAZAS NATURALES	INUNDACIONES	1	1	1
	SISMOS	1	1	1
	TORMENTAS	1	1	1
AMENAZAS A INSTALACIONES	FUEGO	1	1	1
	EXPLOSION	1	1	1
	CAIDA DE ENERGIA	1	1	1
	PERDIDA DE ACCESO	4	1	1
	DAÑO EN PLANTA ELECTRICA	1	1	1
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE	1	1	1
	PROBLEMAS DE TRANSPORTE	1	1	1
AMENAZAS TECNOLOGICAS	VIRUS	2	4	3
	PERDIDA DE DATOS	3	4	4
	FALLAS DE HARDWARE	3	4	4
	FALLAS DE SOFTWARE	3	4	4
	FALLAS DE RED	3	1	4
	FALLAS EN LINEAS TELEFONICAS	1	1	1
	FALLAS EN ANTENAS DE COMUNICACIÓN	1	1	1
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO	4	3	4
	FALLAS EN LAS REPLICAS DE TRANSMILENIO	3	3	4
AMENAZAS SOCIALES	MOTINES	1	1	1
	PROTESTAS	1	1	1
	BOMBAS	1	1	1
	TERRORISMO	1	1	1

TABLA 26

Fuente: norma ISO/IEC 17799:2005

6. ANÁLISIS DEL RIESGO Y SU EVALUACIÓN

El objetivo del análisis del riesgo era identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades. Los riesgos se calculan de la combinación de los valores de los activos, que

expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente

Para efectos de análisis del riesgo y su respectiva evaluación se tomo como base la normatividad ISO/IEC Guide 73:2002, para proceder a realizar el cálculo del riesgo de tal manera que se identificaran más fácilmente los requerimientos de seguridad.

Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización. Todos los riesgos tenían dos factores: unos expresaban el impacto del riesgo si ocurriera; y otro que expresaba la probabilidad de que el riesgo ocurriera.

El factor del impacto del riesgo estuvo basado en la tasación del riesgo. La probabilidad de que el riesgo ocurra se basó en las amenazas y vulnerabilidades y en los valores que se le calcularon. Cabe anotar que el método para el calculo de los riesgos trata de relacionar los factores del “impacto económico de la amenaza” y la probabilidad de ocurrencia de la amenaza”.

Para el caso de las amenazas se estandarizaron a todo nivel para cada uno de los activos de la información según los procesos críticos identificados inicialmente en el estudio; obviamente sin perder el horizonte esquemático de los factores mencionados con anterioridad.

La prioridad según la escala de likert nos permitió realizar una evaluación más adecuada según los riesgos, dándole prelación al “alto” y al “medio alto”; sin dejar a un lado los demás activos.

CALCULO DEL RIESGO PARA ASEGURAMIENTO DEL SERVICIO

		ACTIVO	AMENAZA	IMPACTO DE LA AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACION
ASEGURAMIENTO DEL SERVICIO	ACTIVOS DE INFORMACION	Mensajeria Automatica equipos	Tormentas;Caida de energia; Perdida de acceso, Fallas de Software; Fallas de Hardware; Fallas de red; Fallas en la Replica de TM	4	2	8	3
		Incidencias Operativas	Tormentas;Caida de energia; Perdida de acceso, Fallas de Software; Fallas de Hardware; Fallas en la Replica de TM; Perdida de datos	3	4	12	4
		Configuraciòn dispositivos de memoria	Tormentas;Caida de energia; Perdida de acceso, Fallas de Software; Fallas de Hardware; Fallas de red	4	4	16	4
		Versiones de Firmware	Tormentas;Caida de energia; Perdida de acceso, Fallas de Software; Fallas de Hardware; Fallas de red	4	4	16	4
		Actualización remota	Tormentas;Caida de energia; Perdida de acceso, Fallas de Software; Fallas de Hardware; Perdida de datos	4	1	4	1
	DOCUMENTOS DE PAPEL	Documentacion interna del proceso	Perdida de acceso	1	3	8	3
		Entregas de obras Transmilenio					
		Contrato de concesion					
		Especificaciones tecnicas de equipos					
	ACTIVOS DE SOFTWARE	Windows NT	Perdida de acceso, Daño en Planta Electrica;Perdida de datos;Fallas de Hardware; Fallas de red.	3	3	9	3
		Linux	Perdida de acceso;Perdida de datos;Fallas de Hardware;	4	2	8	3
		Faxila	Perdida de acceso, Daño en Planta Electrica;Fallas de Hardware.	4	2	8	3
		Ovunto	Perdida de acceso, Daño en Planta Electrica;Fallas de Hardware.	4	2	8	3
		NSM	Perdida de acceso, Daño en Planta Electrica;Fallas de Hardware.	4	4	16	4
		Service Desk	Perdida de acceso, Daño en Planta Electrica;Fallas de Hardware; Fallas de red; Perdida de datos	4	5	20	5
		Intranet	Perdida de acceso, Daño en Planta Electrica;Virus;Fallas de Hardware; Fallas de red; Perdida de datos.	5	4	20	5
		Putty	Perdida de acceso, Daño en Planta Electrica;Fallas de Hardware; Fallas de red;	4	1	4	1
	ACTIVOS FISICOS	Equipos de configuracion	Daño en Planta electrica, Fallas de Hardware,	4	5	20	5
		Equipos de recaudo	Tormentas, Caida de energia, Daño en Planta Electrica,Perdida de datos, Fallas de Hadware; Fallas de Software, Fallas en antenas de comunicación.Bombas y terrorismos	5	5	25	5
		Servidores	Tormentas, Caida de energia, Daño en Planta Electrica,Perdida de datos, Fallas de Hadware; Fallas de Software, Fallas en antenas de comunicación.	5	5	25	5
		Banco de pruebas	Daño en Planta Electrica, Fallas de Hadware;	2	1	2	1
	PERSONAL	Auxiliar de Mantenimiento de equipos	Protestas y mala manipulacion de la informacion	3	2	2	1
		Auxiliar Administrativa de activos					
		Auxiliar de Mantenimiento Almacen Satelite					

TABLA 27

Fuente. ISO/IEC Guide 73:2002

CALCULO DEL RIESGO PARA CENTRO DE INFORMACIÓN Y GESTIÓN

		ACTIVO	AMENAZA	IMPACTO DE LA AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICIÓN DEL RIESGO	PRIORIZACION
CENTRO DE INFORMACION Y GESTION	ACTIVOS DE INFORMACION	Base de datos estaciones	Daño en Planta eléctrica, Fallos en CCR; Fallas en replica de TM.	5	4	20	5
		Base de datos transacciones	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas en CCR; Fallas en las replicas de TM.	5	4	20	5
		Base de datos pasadas	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas en CCR; Fallas en las replicas de TM.	5	4	20	5
		Versiones de Software	Perdida de acceso, Daño en Planta Eléctrica; Fallas en hardware, Fallas de Software, fallas en CCR; Fallas en las replicas de TM.	4	3	12	4
		Base de datos usuarios	Perdida de acceso, Daño en Planta Eléctrica; fallas en CCR	5	3	15	4
		Desencole dispositivos de almacenamiento	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas de red,Fallas en CCR	4	4	16	4
		Protocolos IP de equipos de recaudo	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas en CCR	3	1	3	1
		Protocolos IP de equipos de computo	Daño en Planta Eléctrica; pérdida de datos, fallas en CCR	3	1	3	1
		Acceso remoto	Daño en Planta Eléctrica; fallas en CCR	2	1	2	1
		Listas negras	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas en CCR	4	3	12	4
		Listas blancas	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas en CCR	4	3	12	4
	DOCUMENTOS DE PAPEL	Protocolos de software	Perdida de datos	2	1	2	1
		Bitácoras de acceso Centro de Computo					
		Certificado digital					
	ACTIVOS DE SOFTWARE	Oracle Multimaster Replication	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas de red,Fallas en CCR. Fallas en las replicas de TM.	4	2	8	3
		ServiceDev	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.	4	2	8	3
		Toad	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.	4	1	4	1
		Protocolo TCP/IP	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.	4	2	8	3
		Batch	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.	4	1	4	1
		VNP	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.Fallas de red	4	3	12	4
		VNC	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software.Fallas de red	4	3	12	4
		Unicenter	Perdida de acceso, Daño en Planta Eléctrica; pérdida de datos, Fallas en hardware, fallas de Software, fallas de red,Fallas en CCR. Fallas en las replicas de TM.	4	1	4	1
	ACTIVOS FÍSICOS	Centro de computo	Fuego, caída de energía, daño en Planta eléctrica, Virus, pérdida de datos, fallas de Hardware, fallas de Software, fallas de red;Fallas de antenas de comunicación, fallas en CCR, Fallas en las replicas de Transmilenio.	5	3	15	4
		Servidor de archivos de la organización	Caída de energía, daño en Planta eléctrica, Virus, pérdida de datos, fallas de Hardware, fallas de Software, fallas de red.	5	3	15	4
		Servidor base de datos	Caída de energía, daño en Planta eléctrica, Virus, pérdida de datos, fallas de Hardware, fallas de Software, fallas de red.	5	3	15	4
		UCD¨s (Unidad central de datos)	Caída de energía, daño en Planta eléctrica, Virus, pérdida de datos, fallas de Hardware, fallas de Software, fallas de red.Fallas en CCR	5	2	10	3
		Router¨s	Fuego, caída de energía, daño en Planta eléctrica, Fallas de Hardware, fallas de Software.	4	2	8	3
		Switchers	Caída de energía, daño en Planta eléctrica, fallas de Hardware, fallas de Software, fallas en antenas de comunicaciones	4	2	8	3
		Módulos SAM Llaves de seguridad	Fallas de Hardware	3	1	3	1
		Servidor NSM	Caída de energía, daño en Planta eléctrica, virus, Perdida de datos, fallas de Hardware, fallas de Software	2	2	4	1
		Servidor SD	Caída de energía, daño en Planta eléctrica, virus, Perdida de datos, fallas de Hardware, fallas de Software	2	2	4	1
		Controlador de Dominio	Daño en Planta eléctrica, virus, Perdida de datos, fallas de Hardware, fallas de Software	1	2	2	1
	PERSONAL	Analista de Sistemas	Perdida de personal clave	2	4	8	3
		Técnico de Sistemas					
		Auxiliar de Soporte					
		Administrador Base de datos					
		Operario de Informática					

TABLA 28

Fuente. ISO/IEC Guide 73:2002

Una vez efectuado el cálculo del riesgo por cada activo, en relación con su amenaza, se determino cuales son aquellas amenazas cuyos riesgos son los más significativos. Este proceso se denomina evaluación del riesgo.

Para realizar la evaluación del riesgo, se tomo como base los siguientes aspectos tales como:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa
- Posibilidad real de ocurrencia del riesgo
- Posibilidad de interrumpir las actividades de la organización.

A continuación se muestra la planeación estratégica de Angelcom S.A. en el cual se enfoca el estudio y todo el análisis de los riesgos de los sistemas de información.

Para la evaluación del riesgo de los activos de información se realizo un mapa de riesgos para poder identificar los niveles de riesgos aceptables, aquellos riesgos cuyo nivel y estimación de daño es pequeño para la organización y puede aceptarlo como parte de su trabajo cotidiano y, en consecuencia; no se requiere mayor acción. Todos los otros riesgos requieren que la empresa tome acción, y deben estar sujetos al tratamiento de los riesgos y al proceso de toma de decisiones de la Alta Dirección de Angelcom S.A.

Una vez calculados los riesgos, la Alta Dirección estará en capacidad de dictaminar como tratara el riesgo, los cuales estarán influenciados por dos factores:

- El posible impacto si el riesgo se pone en manifiesto

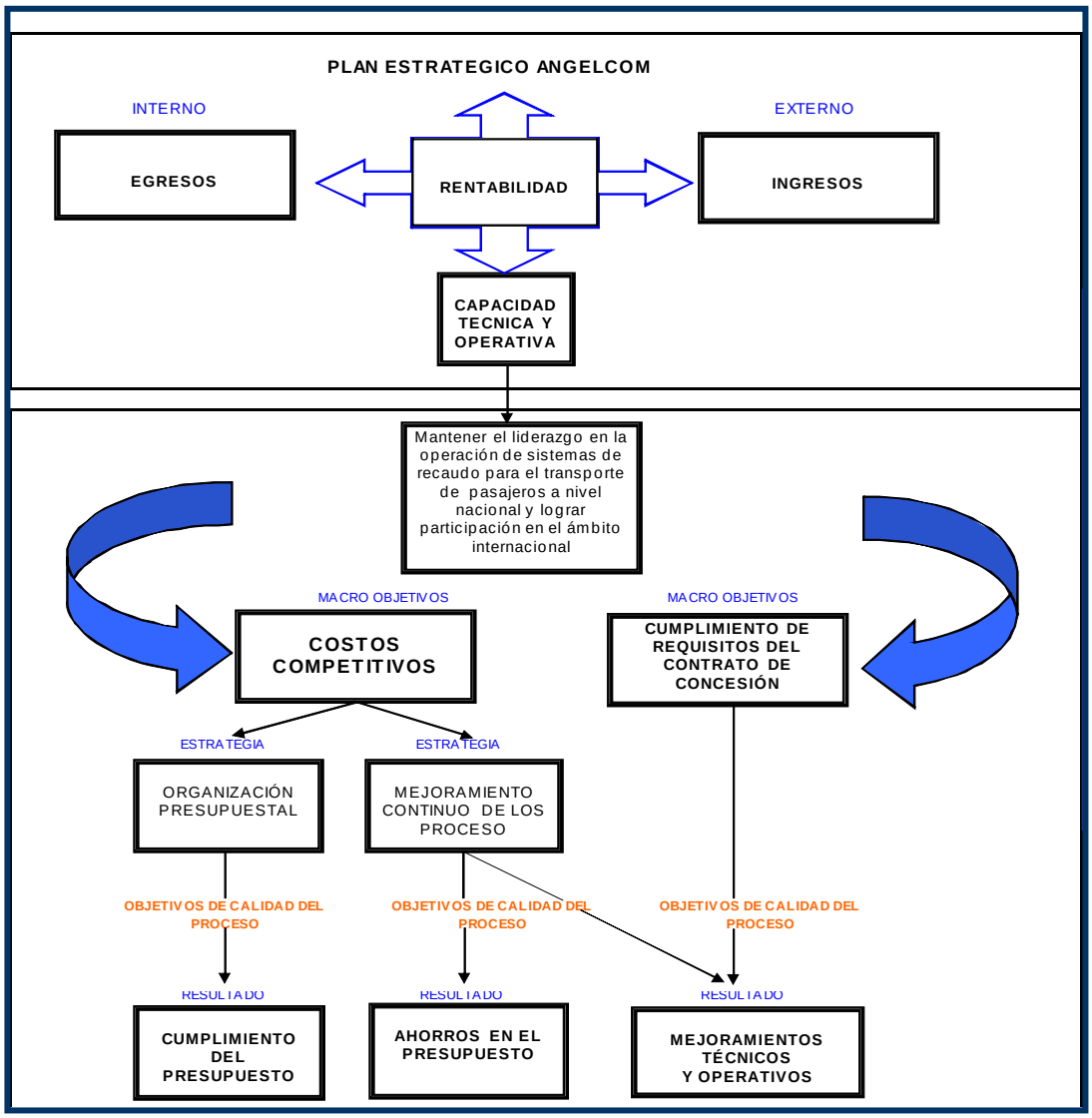

Figura 6. Plan estratégico de Angelcom S.A.

- Qué tan frecuente puede suceder.

Estos factores mencionados darán una idea a la organización de la pérdida esperada si el riesgo ocurriera, y si nada se hiciera para mitigar los riesgos estimados.

Dentro del mapa de riesgos de Angelcom S.A. se identificaron algunos objetivos los cuales se enfocan los activos de información de los procesos críticos.

- Planear la administración y diseño de la arquitectura y control de la Información
- Garantizar la integridad y seguridad de los datos
- Garantizar la disponibilidad y desempeño
- Garantizar la recuperación
- Acompañar el diseño y desarrollo de software que terceros adelantan para la organización
- Cumplimiento del contrato
- Disminución de costos.

Para los riesgos ya identificados dentro del mapa de riesgos, se hizo uso de algunas estrategias para tratar el riesgo específicamente; donde se tenían las siguientes opciones;

1. **REDUCIR EL RIESGO**

Los controles identificados para reducir el riesgo estimado se puede dar de dos maneras: Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza; o reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos.

Para proteger los activos de información de la organización se escogió adoptar cual de estas maneras o una combinación de ambas genera que se tome una decisión de tipo comercial; ya que depende de los requerimientos del negocio, el ambiente y las circunstancias en las cuales la organización necesita operar.

2. ACEPTAR EL RIESGO

En ocasiones se podía presentar la situación en la cual la organización no encontraba los controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias la decisión de aceptar el riesgo y vivir con las consecuencias fue la más adecuada.

3. TRANSFERIR EL RIESGO

La transferencia del riesgo era una opción cuando para la organización era difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante ciertas circunstancias en dado caso que se involucre un requisito del cliente.

4. EVITAR EL RIESGO

Por el modo de evitar los riesgos se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para así evitar la presencia del riesgo. El riesgo se evita por medio de:

- No desarrollar ciertas actividades que involucren la utilización de Internet.
- Mover los activos de un área de riesgo.
- Decidir no procesar información particularmente sensitiva.

Para realizar la evaluación correspondiente a los riesgos se tuvieron en cuenta los siguientes criterios. Ver anexo Mapa de riesgos.

CRITERIOS DE EVALUACIÓN DE RIESGOS

Tipo de riesgo	
EST.	Estratégico
OPV.	Operativo
CUM.	Cumplimiento
FIN.	Financiero
TEC.	Tecnológico
FyC	Fraude y Corrupción

Probabilidad	
Improbable	1
Remoto	2
Ocasional	3
Frecuente	4
Inminente	5

Impacto	
1	Insignificante
5	Leve
10	Moderado
15	Severo
20	Catastófico

Tipo de Control	
Alto nivel	AN
Administrativos	ADM
Sistemas de Información	SI
Físicos	F
Indicadores	I
Segregación de funciones	SF
Procesos y procedimientos	PyP

Criterio de valoración del control	
0	No existe o inexistente
1	Inicial / Ad Hoc
2	Repetible pero intuitivo
3	Control definido y documentado
4	Administrado y medible
5	Mejor práctica

Criterio de aceptación del riesgo	
1 a 19	ACEPTABLE
20 a 29	TOLERABLE
30 a 59	MODERADO
60 a 74	IMPORTANTE
75 a 100	INACEPTABLE

TABLA 29

Fuente: ISO/IEC Guide 73:2002

FASE III: “PLAN DE CONTINUIDAD DEL NEGOCIO” BCP

El BS-25999 es un estándar británico que establece mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta los riesgos a los que se enfrenta una organización midiendo sus impactos de acuerdo a su severidad. El BCP es una metodología que sirve para mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia. Esto implica que un BCP debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio. Bajo este esquema se realizo la metodología del BCP, que se menciona a continuación.

ETAPA 1. BUSINESS IMPACT ANALYSIS (BIA).

.

El Análisis de Impacto del Negocio (BIA –Business Impact Analysis) consiste en técnicas y metodologías que pueden ser usadas para identificar, cuantificar y cualificar los impactos de negocio y sus efectos en una organización en caso de pérdida o interrupción de las actividades de Misión Crítica. Sin embargo, la clave para realizar el Análisis de Impacto del Negocio fue analizar el negocio como un todo más no como componentes, procesos o funciones individuales.

Después de realizado el BIA, se obtendrán como resultados, la identificación y documentación de:

- Objetivos y salidas (servicios y productos).
- Actividades de Misión Crítica, sus dependencias y puntos de falla.
- Impactos y efectos (consecuencias) financieros y no financieros como resultado de una interrupción o pérdida de una o más actividades de misión crítica durante varios periodos de tiempo.
- Los objetivos del BCM para cada actividad de misión crítica y sus dependencias.

- Una priorización mínima y aceptable de la recuperación de los recursos.
- Especifique los procedimientos de respuesta a emergencia.
- Identifique requerimientos de control y autoridad.
- Procedimientos de control y autoridad.
- Respuesta a emergencia y recuperación de heridos.
- Seguridad y recuperación.

PASO 1: IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DE NEGOCIOS.

El propósito de este paso fue identificar las funciones de negocios y procesos que son utilizados en apoyar la misión, visión y objetivos de la organización.

Como primera medida Angelcom S.A**.** es una empresa de ingeniería especializada en proyectos para la Operación y mantenimiento de concesiones de transporte y control de acceso masivo. Fue fundada como entidad nacional e independiente en 1980 incursionando en el campo de las telecomunicaciones, ofreciendo experiencia y versatilidad tecnológica. Con los años y un sostenido crecimiento y consolidación como empresa líder en el sector de la ingeniería de infraestructura de Colombia, incursionó exitosamente en campos como el diseño, construcción, consultoría, inventaría y administración de obras de infraestructura y otros servicios asociados.

En 1999 incursiona en el campo de los sistemas de Recaudo al introducir la tecnología de la Tarjeta Inteligente Sin Contacto (TISC) en el proyecto Transmilenio S.A de la Alcaldía Mayor de Bogotá, lo que hace que Angelcom S.A. transforme sus operaciones y se dedique de manera exclusiva a Operar y Mantener Sistemas de Recaudo bajo plataformas tecnológicas que operan con TISC. En la actualidad atendemos aproximadamente un millón seiscientos mil pasajeros diariamente, efectuando mas de cuatro millones ochocientos mil transacciones en los puntos de venta distribuidos en todas las estaciones y

portales correspondientes a las Fases I y II de Trasmilenio S.A, sistema de transporte masivo que recorre toda la ciudad de Bogotá D.C.

Como parte de esta etapa y a nivel de conocimiento se nombran todos los procesos con sus respectivas funciones; pero para efectos de evaluación de impactos financieros y operacionales se tomaron en cuenta, los procesos críticos y el alcance del Sistema de gestión de seguridad de la información.

FUNCIONES DEL NEGOCIO Y PROCESOS

PROCESO	FUNCIONES
CONCILIACION	CONSOLIDAR Y REPORTAR LA INFORMACION DE LA OPERACIÓN DE RECAUDO
	CONSIGNACION DEL RECAUDO AL ENTE GESTOR
RECAUDO	REALIZAR LAS OPERACIONES DE ADMINISTRACION DE MEDIOS DE PAGO, VENTA Y CONTROL DE ACCESO AL SISTEMA TRANSMILENIO
UNIDAD DE SERVICIO AL CLIENTE	DAR RESPUESTA A LOS REQUERIMIENTOS DE QUEJAS Y RECLAMOS DE LOS USUARIOS DEL SISTEMA TRANSMILENIO
GESTION DE INFORMACION	GARANTIZAR LA CONFIDENCIALIDAD , INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACION GENERADA POR LA OPERACIÓN DE RECAUDO
BASE DE DATOS	PLANIFICACION,DISEÑO DE LA ARQUITECTURA, CONTROL Y ADMINISTRACION DE LA INFORMACION
INFRAESTRUCTURA	ADMINISTRAR Y ASEGURAR LA DISPONIBILIDAD DE LOS ELEMENTOS FISICOS,LOGICOS TALES COMO HARDEARE,SOFTWARE Y SERVICIOS DE COMUNICACIÓN QUE PERMITAN LA OPERACIÓN NORMAL DEL NEGOCIO
INFRAESTRUCTURA E INSTALACIONES	MANTENER LA INFRAESTRUCTURA DEL AREA CONCESIONADA DEL SISTEMA TRANSMILENIO
CENTRO DE ASISTENCIA TECNICA	GESTION, SEGUIMIENTO Y ESCALAMIENTO DE INCIDENTES DE LA PLATAFORMA TECNOLOGICA DE RECAUDO.
MANTENIMIENTO DE EQUIPOS	GARANTIZAR EL FUNCIONAMIENTO FISICO DE LOS EQUIPOS DEL SISTEMA DE RECAUDO.
TALLER DE REPARACIONES	MANTENIMIENTO A LOS DISPOSITIVOS DE LA PLATAFORMA TECNOLOGICA DE RECAUDO Y LOGISTICA Y APROVISIONAMIENTO DE DISPOSTIVOS REQUERIDOS POR LA OPERACIÓN.
GESTION HUMANA	VINCULAR Y MANTENER EL PERSONAL IDONEO CONFORME A LAS NECESIDAD PROPIAS DEL CLIENTE.
SERVICIOS GENERALES	ADQUISICION DE BIENES Y SERVICIOS AL MENOR COSTO Y A LAS MEJORES CONDICIONES COMERCIALES
FINANCIERA	ADMINISTRAR LOS RECURSOS FINANCIEROS PARA GARANTIZAR LA OPERACIÓN CONFORME A LOS REQUISITOS LEGALES Y REGLAMENTARIOS
MEJORAMIENTO CONTINUO	MANTENER EL SISTEMA DE GESTION DE CALIDAD

TABLA 30

Fuente: Caracterizaciones del cada proceso SGC.

PASO 2: EVALUACIÓN DE LOS IMPACTOS FINANCIEROS Y OPERACIONALES

IMPACTOS FINANCIEROS

La magnitud financiera de la severidad de los impactos de una interrupción debía medirse; por el cual para esta medición se tomo como base la siguiente pregunta: ¿Cuáles serian la magnitud y la severidad de las pérdidas financieras si el proceso fuese interrumpido después de un desastre?

Para la medición de los impactos financieros se tuvo en cuenta las multas establecidas por el contrato de concesión; y por ende la base de severidad, basada en el valor de la pérdida monetaria.

Transmilenio S.A. verificará el cumplimiento de la totalidad de los parámetros, requisitos, obligaciones y responsabilidades exigibles al concesionario en virtud de lo dispuesto en el contrato de concesión. Si el concesionario no cumple con cualquiera de los parámetros establecidos en cuanto a seguridad de la información con TransMilenio S.A o con cualquiera de los requisitos, obligaciones y responsabilidades que le han sido asignados en el presente contrato, a partir de la fecha en que cada obligación se hace exigible comenzará a causarse una multa diaria de acuerdo con lo previsto en las cláusulas. Sin subordinación ni sujeta a condición alguna diferente de la ocurrencia de los supuestos fácticos que dan lugar al nacimiento y exigibilidad de la multa, y sin requerirse declaración alguna de parte de Transmilenio S.A. o de otra autoridad judicial o extrajudicial de cualquier naturaleza.

En todo caso, en ningún evento se causarán multas por un valor total acumulado que supere del diez por ciento (10%) del valor total de los ingresos que por todo

concepto perciba el concesionario con ocasión del contrato, para el periodo semanal en el que se haya causado la sanción correspondiente.

Para realizar dicha medición se utilizo la siguiente escala

- Nivel de Severidad 0: Impacto 0
- Nivel de Severidad 1: Menor impacto
- Nivel de Severidad 2: Impacto intermedio
- Nivel de Severidad 3: Impacto mayor.

IMPACTOS FINANCIEROS Y NIVELES DE SEVERIDAD POR SUBPROCESOS

PROCESO	FUNCIONES	MAGNITUD DE PÈRDIDA FINANCIERA (Total)	MAGNITUD DE PÈRDIDA FINANCIERA (Diaria)	NIVEL DE SEVERIDAD
GESTION DE INFORMACION	GARANTIZAR LA CONFIDENCIALIDAD , INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACION GENERADA POR LA OPERACIÓN DE RECAUDO	$ 1.560.000.000	$ 52.000.000	3
BASE DE DATOS	PLANIFICACION,DISEÑO DE LA ARQUITECTURA, CONTROL Y ADMINISTRACION DE LA INFORMACION	$ 780.000.000	$ 26.000.000	2
INFRAESTRUCTURA	ADMINISTRAR Y ASEGURAR LA DISPONIBILIDAD DE LOS ELEMENTOS FISICOS,LOGICOS TALES COMO HARDEARE,SOFTWARE Y SERVICIOS DE COMUNICACIÓN QUE PERMITAN LA OPERACIÓN NORMAL DEL NEGOCIO	$ 156.000.000	$ 5.200.000	3
CENTRO DE ASISTENCIA TECNICA	GESTION, SEGUIMIENTO Y ESCALAMIENTO DE INCIDENTES DE LA PLATAFORMA TECNOLOGICA DE RECAUDO.	$ 7.800.000	$ 260.000	1
MANTENIMIENTO DE EQUIPOS	GARANTIZAR EL FUNCIONAMIENTO FISICO DE LOS EQUIPOS DEL SISTEMA DE RECAUDO.	$ 504.400.000	$ 16.813.333	2
TALLER DE REPARACIONES	MANTENIMIENTO A LOS DISPOSITIVOS DE LA PLATAFORMA TECNOLOGICA DE RECAUDO Y LOGISTICA Y APROVISIONAMIENTO DE DISPOSTIVOS REQUERIDOS POR LA OPERACIÓN.	$ 7.800.000	$ 260.000	1

TABLA 31

Fuente: Contrato de concesión.

I

IMPACTOS OPERACIONALES:

La medición de los impactos operacionales evalúa el impacto negativo de una interrupción, en varios aspectos de las operaciones del negocio.

		IMPACTOS OPERACIONALES				
PROCESO	FUNCIONES	FLUJO DE CAJA	CONFIANZA INVERSION	CUMPLIMIENTO CONTRACTUAL	COSTOS COMPETITIVOS	SATISFACCION DEL CLIENTE
GESTION DE INFORMACION	GARANTIZAR LA CONFIDENCIALIDAD , INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACION GENERADA POR LA OPERACIÓN DE RECAUDO	4	3	5	4	5
BASE DE DATOS	PLANIFICACION,DISEÑO DE LA ARQUITECTURA, CONTROL Y ADMINISTRACION DE LA INFORMACION	4	3	5	4	3
INFRAESTRUCTURA	ADMINISTRAR Y ASEGURAR LA DISPONIBILIDAD DE LOS ELEMENTOS FISICOS,LOGICOS TALES COMO HARDEARE,SOFTWARE Y SERVICIOS DE COMUNICACIÓN QUE PERMITAN LA OPERACIÓN NORMAL DEL NEGOCIO	4	2	5	4	5
CENTRO DE ASISTENCIA TECNICA	GESTION, SEGUIMIENTO Y ESCALAMIENTO DE INCIDENTES DE LA PLATAFORMA TECNOLOGICA DE RECAUDO.	1	1	4	1	4
MANTENIMIENTO DE EQUIPOS	GARANTIZAR EL FUNCIONAMIENTO FISICO DE LOS EQUIPOS DEL SISTEMA DE RECAUDO.	5	1	5	4	5
TALLER DE REPARACIONES	MANTENIMIENTO A LOS DISPOSITIVOS DE LA PLATAFORMA TECNOLOGICA DE RECAUDO Y LOGISTICA Y APROVISIONAMIENTO DE DISPOSTIVOS REQUERIDOS POR LA OPERACIÓN.	5	1	4	5	5

ESCALA	MUY BAJO	BAJO	MEDIO	ALTO	MEDIO ALTO
VALOR	1	2	3	4	5
PORCENTAJE	5	1	3	10	11
	17%	3%	10%	33%	37%

TABLA 32

Fuente: Alberto G. Alexander. Óptica ISO 27001:2005

PASO 3: ESTABLECIMIENTO DE LOS TIEMPOS DE RECUPERACIÓN.

Los requerimientos de los tiempos de recuperación consisten en una serie de componentes que tienen que ver con el tiempo disponible para recuperarse de una alteración. Para evaluar los MTD se tuvo en cuenta la Guide to Business Continuity Planning de Barnes James, 2001. Esta guía establece el método para cuantificar los MTD y su recuperación en el tiempo.

Estos tiempos de recuperación se ilustran a continuación:

MTD: Este tiempo representa el periodo máximo de tiempo de inactividad que puede tolerar la organización, sin entrar en un colapso financiero y operacional.

PRIORIDADES DE RECUPERACIÓN PARA PROCESOS CRÍTICOS DE ANGELCOM S.A

PROCESO	FUNCIONES	MTD (Dias)	PRIORIDAD DE RECUPERACION
GESTION DE INFORMACION	GARANTIZAR LA CONFIDENCIALIDAD , INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACION GENERADA POR LA OPERACIÓN DE RECAUDO	1	5
BASE DE DATOS	PLANIFICACION,DISEÑO DE LA ARQUITECTURA, CONTROL Y ADMINISTRACION DE LA INFORMACION	1	4
INFRAESTRUCTURA	ADMINISTRAR Y ASEGURAR LA DISPONIBILIDAD DE LOS ELEMENTOS FISICOS,LOGICOS TALES COMO HARDEARE,SOFTWARE Y SERVICIOS DE COMUNICACIÓN QUE PERMITAN LA OPERACIÓN NORMAL DEL NEGOCIO	3	4
CENTRO DE ASISTENCIA TECNICA	GESTION, SEGUIMIENTO Y ESCALAMIENTO DE INCIDENTES DE LA PLATAFORMA TECNOLOGICA DE RECAUDO.	2	3
MANTENIMIENTO DE EQUIPOS	GARANTIZAR EL FUNCIONAMIENTO FISICO DE LOS EQUIPOS DEL SISTEMA DE RECAUDO.	1	5
TALLER DE REPARACIONES	MANTENIMIENTO A LOS DISPOSITIVOS DE LA PLATAFORMA TECNOLOGICA DE RECAUDO Y LOGISTICA Y APROVISIONAMIENTO DE DISPOSTIVOS REQUERIDOS POR LA OPERACIÓN.	1	1

TABLA 33

Fuente: Alberto G. Alexander. Óptica ISO 27001:2005

Dados los MTD de los procesos críticos, puede establecerse una prioridad para su recuperación. Un proceso critico que tiene un MTD menor comparado con otro, tendrá mayor prioridad para la recuperación. Para este caso Taller de Reparaciones tendría un mayor nivel de prioridad.

CÁLCULO EXPOSICIÓN DEL RIESGO SEGÚN LAS AMENAZAS

		SEVERIDAD				COBERTURA						EXPOSICION DEL RIESGO %
AMENAZAS		NO APLICA	BUENO (10)	MODERADA (50)	ALTA (100)	0-19	20-39	40-59	60-79	80-99	100	
AMENAZAS NATURALES	INUNDACIONES	0				0						0
	SISMOS		10			8						9,2
	TORMENTAS				100					85		15
AMENAZAS A INSTALACIONES	FUEGO		10				30					7
	EXPLOSION			50					60			20
	CAIDA DE ENERGIA				100						100	100
	PERDIDA DE ACCESO			50						80		10
	DAÑO EN PLANTA ELECTRICA				100					85		15
AMENAZAS HUMANAS	PERDIDA DE PERSONAL CLAVE			50					60			20
	PROBLEMAS DE TRANSPORTE	0				8						0
AMENAZAS TECNOLOGICAS	VIRUS				100					90		10
	PERDIDA DE DATOS				100						100	100
	FALLAS DE HARDWARE				100						100	100
	FALLAS DE SOFTWARE				100						100	100
	FALLAS DE RED			50			35					32,5
	FALLAS EN LINEAS TELEFONICAS		10			5						9,5
	FALLAS EN ANTENAS DE COMUNICACIÓN			50					75			12,5
AMENAZAS OPERACIONALES	FALLAS EN LOS EQUIPOS DE RECAUDO				100						100	100
	FALLAS EN LAS REPLICAS DE TRANSMILENIO		10			19						8,1
AMENAZAS SOCIALES	MOTINES		10			10						9
	PROTESTAS			50		10						45
	BOMBAS			50				45				27,5
	TERRORISMO			50						80		100

TABLA 34

Fuente: Alberto G. Alexander. Óptica ISO 27001:2005

ETAPA II: GESTIÓN DEL RIESGO.

El objetivo de la evaluación de riesgos es identificar las amenazas internas y externas, incluyendo concentraciones de riesgo, que pueden causar la interrupción o pérdida de la actividades críticas de una organización, así como la probabilidad (o frecuencia) de que ocurra una amenaza y cómo es vulnerable una organización a varios tipos de amenazas permitiendo su gestión de priorización y control para formar una base en la que se establezca un programa de control y un plan de acción de gestión de riesgo.

Para realizar una evaluación y control de riesgos se debe tener en cuenta lo siguiente:

- Identificar riesgos
- Análisis/Evaluación de riesgos
- Gestión y Control de riesgos

Después de realizar la evaluación y el control de riesgos los resultados obtenidos incluyen la identificación y documentación de:

- La probabilidad de ocurrencia, en la organización, a un tipo específico de amenaza.
- Concentración de riesgos donde el número de actividades de Misión Crítica es localizado dentro del mismo edificio o en el mismo lugar.
- Una evaluación y análisis de riesgos (combinado con un Análisis de Impacto del Negocio - BIA).
- Una estrategia de gestión de control de riesgo y plan de acción. El enfoque de priorización del BCM y control de riesgos.

Como soporte a la gestión del riesgo, se muestra el mapa de riesgos establecido, para identificar los literales mencionados con anterioridad. Ver anexo 2.

4. CONCLUSIONES

El Modelo del Diseño del Sistema de Gestión de la Seguridad Informática bajo el contexto de una organización inteligente, tiene como objetivo la disminución de la incertidumbre y la complejidad en la situación en que se encuentra la seguridad de la información, los cinco niveles que lo integran no se limitan exclusivamente a describir factores que influyen sobre ella, como los gerenciales, el análisis de gestión de riesgo, la planificación estratégica y la cultura organizacional, entre otros. Este modelo incorpora herramientas de una organización alineada con el concepto de la normatividad ISO 27001:2005 e ISO/ICE 17799:2005, característica que permite derrumbar algunos mitos y creencias que afectan la instrumentación de acciones que reducen el riesgo potencial de materializarse una amenaza, dada una vulnerabilidad asociada a un activo informático. En efecto, las disciplinas de Angelcom S.A. le dan valor agregado al modelo propuesto, generan sinergia.

El problema de la inseguridad informática no se resuelve únicamente al identificar los servicios de seguridad a proteger, las herramientas de seguridad de las TIC’s, la operacionalización de las políticas de seguridad y las normas, la situación es compleja, trasciende los aspectos tecnológicos, involucra el trabajo en conjunto de los trabajadores encargados de la seguridad, el desarrollo continuo de nuevas actitudes y aptitudes, la aplicación del pensamiento sistémico, un factor crítico al incorporar el dogma de las organizaciones inteligentes, sus valores éticos, la visión compartida y los modelos mentales bajo una perspectiva de la seguridad de la información. Sin embargo, en muchas organizaciones, los gerentes y el personal encargado de la seguridad de la información poseen un modelo mental que impide a las organizaciones alcanzar un mayor nivel de madurez en el manejo de la situación.

Otras posibles conclusiones del presente estudio se pueden dar bajo los siguientes puntos:

- Hay decisiones respecto al cumplimiento de políticas dentro SGSI que deben ser de carácter jerárquico, impulsado por la Alta Direccion, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa. Bajo esta afirmación, la Alta Dirección de Angelcom no garantizo la participación activa de todos los lideres del proceso, retrasando las actividades programadas y el objetivo previamente dicho: Analizar y evaluar los riesgos a los que estaban sujetos los activos de la información de Angelcom S.A

- Un SGSI no puede ser implantado por simple requisito sino siempre buscando objetivos claros que agreguen valor a la organización. Toda nueva implementación en pro de mejoras en la seguridad de la información debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI, sin embargo el poco interés de la organización de conocer los riesgos a los cuales están expuestos, conllevó a restringir y al no acceder a la información requerida en el presente estudio..

- El eslabón más débil de la cadena son las personas, por lo tanto dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento. Dentro del análisis se pudo evidenciar que uno de las factores que afectan la disponibilidad e integridad de la información son por fallas del personal, ya que en gran parte la manipulación de la información no esta dada por sistemas operativos óptimos, lo cual genera errores de configuración, de transaccionalidades mal ejecutadas y saltos de información.

5. RECOMENDACIONES

Dentro del desarrollo del proyecto se pudo evidenciar algunas falencias las cuales pueden ser cruciales en el momento de querer implementar un Sistema de Gestión de Seguridad de la Información, estas recomendaciones se basan bajo el marco referencial ISO 2007:2005 y de la recolección de datos establecidos como metodología.

- **Definición de Funciones y Responsabilidades**

Una de las principales amenazas de Angelcom S.A es el acceso de usuarios no autorizados (internos o externos) que puedan consultar, modificar, borrar e incluso robar información a la que no deberían acceder. El usuario del sistema de información debe ser informado de forma clara y precisa acerca de sus funciones y obligaciones en el tratamiento de los datos.

Implantación de Medidas

Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores.

- **Validez jurídica de las evidencias**

La mayoría de las actuaciones que se llevan a cabo en el marco de la seguridad de la información en Angelcom S.A. cumplen con el objetivo de disuadir al usuario, interno o externo, de realizar actuaciones no autorizadas, o bien de impedir la ejecución de dichas actuaciones. No obstante, si se produce una incidencia relacionada con la seguridad de la información, siempre se piensa que las pruebas incriminarán al infractor; pero este extremo resulta del todo inútil si no se ha

contemplado esta finalidad en el diseño de las políticas de seguridad de la organización.
Establecer en todas las medidas de seguridad adoptadas el carácter de prueba para poder demostrar posibles incumplimientos con las normas establecidas en el uso de la información de la organización.

Implantación de Medidas

Será objetivo de un grupo de trabajo multidisciplinar, (en el que se debe contar con apoyo jurídico, técnico y organizativo -definido en la presente guía como comité de seguridad), dotar de validez jurídica a las pruebas de incumplimiento de las medidas de seguridad definidas sobre la seguridad de la información y según contrato de concesión.

- **Comunicaciones de información con terceros**

Uno de los procesos que más amenazas puede generar en las relaciones con los terceros es el intercambio de información.
El envío de datos a través de soportes (llaves de seguridad o USB's) o redes de telecomunicaciones (correo electrónico, mensajería), generan amenazas a la integridad de los datos, pero también a la confidencialidad de los mismos. Evitar pérdidas, intercepciones o alteraciones de la información, es una prioridad para que Angelcom S.A, evalué y las tenga presente. El procedimiento actual es muy específico y no se encuentra documentado.

Implantación de Medidas
Los subprocesos de Centro de Información y Gestión deben estar perfectamente definidos y regulados en los contratos de prestación de servicios. De forma adicional, se deben establecer normas y mecanismos que permitan realizar

comunicaciones de información de forma segura, dentro de la organización y con terceros.
Dichas normas deben estar recogidas formalmente y ser difundidas a todos los implicados en el envío o recepción de información

- **Contratos con terceros**

La evolución de los sistemas de información permiten un mayor grado de subcontratación a las organizaciones, asesorías fiscales y laborales, empresas que ofrecen hosting (alquileres) de servidores o páginas web, copias de seguridad realizadas en remoto, etc, son algunos de la larga lista de servicios que se pueden contratar. Si estos terceros no conocen la política de seguridad de la organización, no podrán ser capaces de prestar los servicios contratados con las garantías mínimas exigidas, es pues recomendable y en algún caso imprescindible, regular formalmente los servicios que involucren a personal o recursos externos a la organización.
Tratar los datos de una forma distinta a la acordada, realizar un uso de los mismos para otra finalidad distinta a la inicialmente contratada, no aplicar las medidas de seguridad exigidas, no informar a los usuarios acerca de su deber de secreto, son aspectos que deben estar perfectamente definidos al regular el contrato de prestación de servicios.

Implantación de Medidas

Todas las relaciones con empresas y organizaciones ajenas, que impliquen el acceso a los datos e información propios de la organización deben estar reguladas mediante contrato, estos contratos deberán contemplar como mínimo:

- La identificación de todas las personas físicas y jurídicas que tendrán acceso a la información.
- La finalidad de la prestación de servicios.
- Los mecanismos de intercambio de información.

- Las medidas de seguridad a aplicar a los datos.
- La obligación de mantener el deber de secreto y de informar del mismo a todos los usuarios que puedan acceder a la información.
- Las condiciones para la finalización del contrato, incluyendo mención específica a las acciones de devolución o destrucción de la información objeto del contrato.

La concientización de Angelcom S.A. es un pilar fundamental de la norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Existen mecanismos como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

Las organizaciones deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas.

Finalmente, la implementación del Diseño del Sistema de Gestión de Seguridad de la información requiere una participación activa y completa a nivel estratégico. Su papel tiene que ser protagónico en su implementación. Durante el desarrollo del presente estudio se pudo evidenciar una disminución en el compromiso de la Alta Dirección por el cual no se facilito realizar el proyecto en los tiempos asignados; por tanto la correcta implementación del modelo de cualquier empresa debe seguir pasos metodológicos comprobados y consistentes, que den resultados comparables y reproducibles, y dicho con estas palabras se debe tener mayor dedicación, y esfuerzos compartidos para que un futuro se puede pensar en una posible certificación en ISO 27001:2005.

BIBLIOGRAFÍA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma ISO/IEC FDIS 27001:2005.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma ISO/IEC 17799:2005.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN Norma ISO Guide 73:2002

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN Norma ISO 13335:2004

ALBERTO G. Alexander. Primera Edición. Colombia, 2007. Diseño de un Sistema de Gestión de Seguridad de Información.

DÍAZ PIRAQUIVE, Flor Nancy. Segunda Edición. Madrid, España.2004. Principales estándares para la seguridad de la información IT

BARNES, James. Primera Edición. Londres Wiley.2001. A Guide to Business Continuity Planning.

PRICE WATER HOUSE COOPERS (2009) Global State of Information Security Study.

ESTÁNDAR BRITÁNICO BS 25999. Plan de Continuidad del Negocio – o BCM (Business Continuity Planning).

INFOGRAFÍA

- http://es.wikipedia.org/wiki/Información
- http://www.segu-info.com.ar/logica/seguridadlogica.htm.
- http:/www.seguridadcorporativa.org
- http://www.seguridadenlared.org/es/index5esp
- www.bsi.com British Standard Institute
- www.eumed.net/libros/introduccionalametodologiadelainformacion
- www.oecd.org. OECD 2002. Guía de administración de riesgos de sistemas de información y redes.
- www.hacktimes.com. Daniel P.F a.k.a metal at/dot Análisis y modelado de amenazas y vulnerabilidades.