Trabajo Fin Master- Propuesta para la Planeación e Implementación de un SGSI basado en la ISO/IEC 27001:2005 para una empresa de telecomunicaciones

Autor: Héctor Fernando Vargas Montoya

Consultor/Tutor: ANTONIO JOSE SEGOVIA HENARES

Trabajo Fin de Master – TFM

UOC - Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones- MISTIC

Junio 2014

Contenido

Lista de gráficas

Lista de tablas

Resumen

El presente documento corresponde al Trabajo Final del Master – TFM del "Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones- MISTIC" de la universitat Oberta de Catalunya, Universitat Rovira i Virgili y la Universitat Autonoma de Barcelona, el cual se fundamenta en la propuesta de planeación y diseño de un sistema de gestión de seguridad SGSI así como la implementación de algunos de los elementos, basado en la norma ISO/IEC 27001:2005 y su anexo la ISO 27002, dicho proyecto está enmarcado para una empresa de telecomunicaciones en Colombia y estará proyectado acorde al alcance y la declaración de aplicabilidad.

El SGSI sigue el proceso/ciclo de Deming (Planear-Hacer-Verificar-Actuar) y dentro de éste marco de referencia, se pretende conocer el sector de las telecomunicaciones (y sus servicios asociados) y dar una aplicabilidad de lo que es la implantación de un SGSI en pro de la protección de la información. De igual manera, en la propuesta de implementación de controles se tendrán en cuenta la normatividad y legislación actual existente en Colombia, construyendo así un sistema basado en la mejora continua.

Limitaciones

En el presente documento se entregan los elementos de planeación, algunos elementos del SGSI serán implementados (más no es su totalidad), dado que esto dependerá del apoyo de la alta gerencia, de los recursos humanos y económicos. La estrategia de implementación está basada en la "implementación por ganancias tempranas", esto es, se implementarían algunos controles a los cuales no necesariamente se le asocie un presupuesto y sean rápidos de implementar. Al final del documento se indicarán cuales fueron implementados o están en ese proceso.

Introducción

Una empresa de telecomunicaciones tiene múltiples variantes en servicios y productos (multi-servicio) que son brindados a los diferentes clientes, los servicios de telecomunicaciones abarcan desde brindar acceso hacia Internet desde los hogares y empresas, pasando por conexiones entre redes hasta servicios de telefonía fija y móvil, voz sobre IP y portales Web (Hosting), entre otros. Dentro de todo el proceso de venta, aprovisionamiento del servicio, facturación y recaudo, se puede observar cómo los sistemas de información son parte fundamental dentro de los procesos (cadena de valor), de modo que las tareas puedan ser lo más automáticas posibles, con ello, generar valor para la empresa.

Teniendo en cuenta los diferentes sistemas de TI y la información que allí se maneja, es necesario buscar los mejores mecanismos que permitan la protección de ésta información contra modificaciones, alteraciones, copia, y/o borrado no autorizado, reduciendo los

riesgos de exposición, es así como se hace necesario establecer un contexto de trabajo que logre proteger dicha información y para ello se vuelve necesario la implementación de un SGSI cuyo fundamento es permitir que la información esté protegida, conservado su confidencialidad, disponibilidad e integridad, logrando esto desde una adecuada gestión del riesgos.

Teniendo en cuenta que la norma ISO/IEC 2001:2005 es una de las mejores guías de seguridad, en éste trabajo se pretende entregar una propuesta de cómo se implementaría un SGSI para una empresa de telecomunicaciones bajo dicha norma (así mismo se implementarán algunos elementos acá descritos) y limitado por el alcance hacia los sistemas de información que soportan los procesos críticos, adicional a esto, enmarcado en la legislación vigente en Colombia.

1. Contextualización: Análisis de la empresa

A continuación se da el contexto general de la empresa:

a. Descripción y servicios

El objeto comercial de la empresa de telecomunicaciones en Colombia es brindar servicios tecnológicos a nivel nacional y a diferentes segmentos del mercado, sus clientes son el segmento de hogares residenciales, Pymes y grandes empresas.

Tiene presencia en las ciudades de Bogotá, Medellín, Cali, Barranquilla, Manizales, Pereira, Cartagena y Cúcuta.

Para el segmento de hogares se ofrecen los siguientes servicios:

- *Televisión por cable: Con una amplia gama de canales (grilla) nacionales e internacionales, brinda a demás canales en alta definición (HD).*
- *Telefonía básica, con servicios de llamadas nacionales e internacionales.*
- *Acceso a Internet de alta velocidad, a través de tecnologías como DSL y Cablemodem.*
- *Tarjetas prepagos.*

Para el segmento de las empresas se ofrecen los siguientes servicios:

- *Soluciones de Internet Data Center – IDC, con las diferentes modalidades en hosting (publicación de sitios Web) y collocation (alquiler de espacios físicos con aire acondicionado y potencia).*
- *Servicios de voz: a través de troncales IP (VoIP/ToIP).*
- *Conectividad entre empresas.*
- *Internet y televisión empresarial*
- *Servicios profesionales de consultoría en tecnología.*

- *Sistemas de video conferencia.*
- *Servicios de Contac Center – call center*

De igual manera tiene sus sistemas de peticiones, quejas y reclamos – PRQ y da cumplimiento a la legislación en telecomunicaciones entregada por el ministerio de las TIC de la republica de Colombia.

Para la empresa de telecomunicaciones es fundamental mantener relaciones de largo plazo con sus proveedores, contratistas y aliados, brindando de manera oportuna, segura y confiable los diferentes servicios de telecomunicaciones a nivel nacional, cumpliendo además, con la responsabilidad social hacia las TIC.

Se conocido que los diferentes sectores y en espacial en sector empresarial, han estado demandando servicios que cierto grado de seguridad y confiabilidad, teniendo en cuenta que los clientes potenciales requieren de la tecnología para sus objetos de negocio. Así mismo, la regulación actual indica unas exigencias en temas de seguridad y protección de información altos que son necesarios cumplir.

b. Procesos internos

Para brindar los diferentes servicios de telecomunicaciones, el mapa de procesos se basa bajo la metodología e-TOM[1] (por sus siglas en ingles "Enhanced Telecom Operations Map") y el mapa de operaciones de telecomunicaciones mejorado ITU-M.3050[2], para lo cual es ajustada acorde a las necesidades de la empresa y para ello, se ha definido el siguiente diagrama de procesos de alto nivel:

[1] The Business Process Framework (eTOM): Framework de procesos para empresas de Telecomunicaciones.
[2] Unión internacional de Telecomunicaciones – ITU-T, M.3050

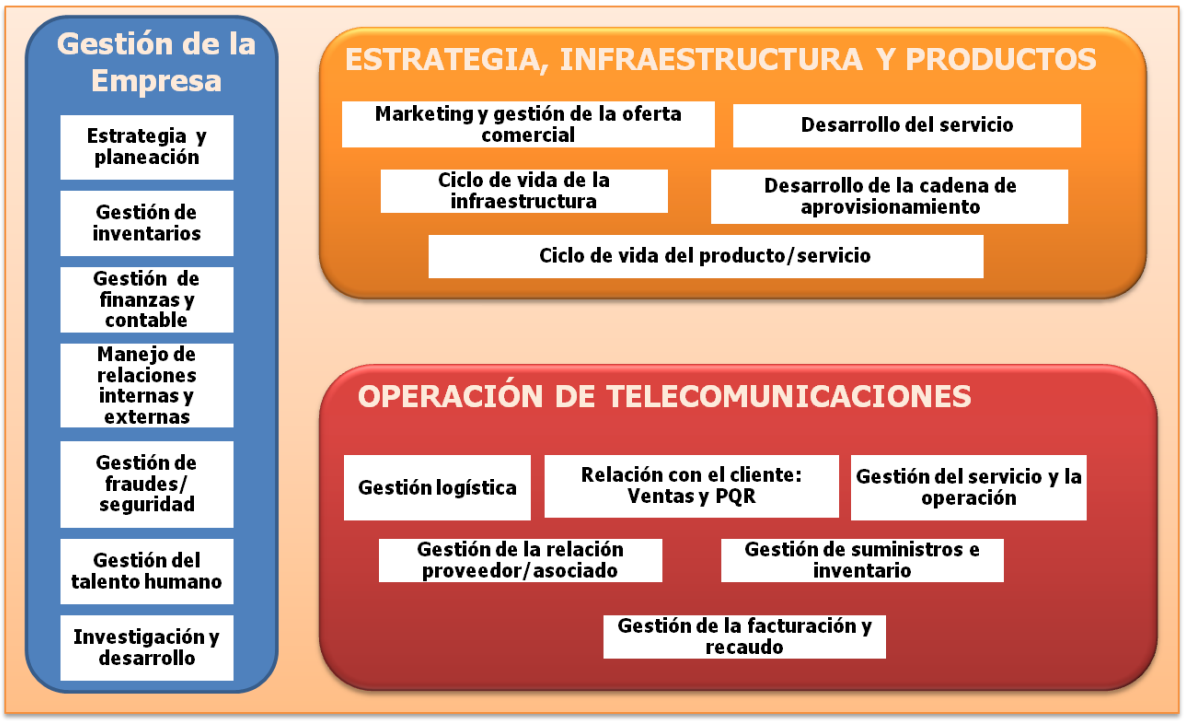

Figura 1: Mapa de procesos de alto nivel.
Elaborado con datos propios

Dentro de los procesos podemos destacar los siguientes, los cuales son considerados de misión crítica para los servicios brindados al segmento de Hogares:

- *La interacción con los clientes inician desde la pre-venta y venta de los productos y servicios desde el CRM (Customer relationship management).*
- *El aprovisionamiento de servicios se hace desde plataformas tipo OSS (Operations Support Systems), el cual es un sistemas de información usado por las empresas operadoras de telecomunicaciones para aprovisionar y desaprovisionar los diferentes servicios.*
- *Se hace un agendamiento con los clientes para realizar una visita domiciliaría, donde se hace una revisión o se hace una instalación de a red cableada, incluyendo el CPE (Customer Premises Equipment) de conexión (equipo terminal que se instala en los hogares).*
- *Una vez culminada la cita, ésta se cierra en línea a través de un portal Web o al final del día sobre el sistema de Información.*
- *Se inicia entonces el proceso de facturación, de modo que le llegue de manera oportuna la factura a cada cliente, éste tiene 2 posibilidades: que llegue de manera física o en línea, a través de un portal Web destinado para ello y a través de las notificaciones por correo electrónico. Todo el proceso se hace a través del sistema propio de facturación y a través de los portales Web.*
- *El siguiente paso es el sistema de recaudo, el cual tiene múltiples variantes: Se puede realizar de manera física en algunos bancos nacionales y/o locales, a través*

de transferencia electrónica con pago con tarjeta o a través del portal Web a través del sistema de comercio electrónico.

- *La etapa final y como lo dispone el Ministerio de las tecnologías de Información y Comunicaciones en Colombia (MinTIC), se podría ejecutar eventualmente los procesos de PQR (Peticiones, quejas y reclamos) hacia los clientes, esto, realizado a través del CRM.*
- *De manera consecuente, una vez se culmina el sistema de facturación y recaudo, se hace la interacción con el sistema financiero a través de la ERP, el cual llevara la contabilidad respectiva.*

Para éstos procesos, los sistemas de información son fundamentales para soportar el negocio, dentro de los sistemas de información están los siguientes:

- **Ventas y PQR***: Se gestiona desde el CRM*
- **Facturación y recaudo***: Desde el aplicativo de facturación, el cual cuenta con módulos para la liquidación del recaudo.*
- **Aprovisionamiento de soluciones***: Se hace desde el OSM o sistema de aprovisionamiento en telecomunicaciones, el sistema una vez ejecuta varias acciones:*
  - *El CRM lanza la petición de aprovisionamiento o retiro de clientes.*
  - *El OSM hace una validación y reserva en el inventario de posibles equipos a instalar.*
  - *Hace una activación automática sobre el sistema que maneja el servicio (Banda ancha, televisión, telefonía, u otro servicio).*
  - *Cuando el personal de campo ejecuta la actividad y hace el cierre de la orden de instalación, el OSM da por cumplido el aprovisionamiento, envía notificación al CRM y al facturador para que inicie el proceso de facturación y recaudo respectivo.*
- **Sistemas Financiero sobre la ERP***: Donde está, entre otros, la contabilidad.*
- **Sitios Web***: Para cerrar las instalaciones y/o visitas a los clientes y para la gestión de pagos en línea o e-comerce.*

2. Justificación

La información, como fuente fundamental en las organizaciones debe tener un tratamiento optimo, de modo que la alineación estratégica, toma de decisiones y el contacto con los clientes, tengan un nivel de certeza lo más real posible. Para lograr esto, es necesario identificar, conocer y reconocer la diferente información con que se cuenta y sobre ésta, definir un nivel de criticidad para poder dar un nivel de protección adecuada.

Si no tenemos información oportuna, veraz y ágil, muchos de los clientes se estarán retirando o cancelando los servicios, dado que, no se contaría, por ejemplo, con información precisa a la hora de visitar a los clientes para la instalación (haciendo perder

tiempos innecesarios a éstos y costos adicionales al tener que volver a visitar). Ahora bien, si la información es parte fundamental, ¿qué hacen las organizaciones para protegerla?

Figura 2: Distribución proceso evaluación de riesgos en las empresas
Asociación Colombiana de Ingenieros de Sistemas – ACIS. 2013. Tomado de http://www.acis.org.co/index.php?id=332

Según la V encuesta anual latinoamericana de seguridad de la información, para el 2013 el 48% de las empresas encuestadas en Latinoamérica no poseían un proceso formal de gestión del riesgo, por consiguiente, existe la posibilidad que éste número de empresas no tenga una adecuada gestión de la seguridad y los posibles impactos negativos a la información.

Así mismo, dentro de la misma encuesta se encontró que un 52.59% de las empresas encuestadas no tienen un proceso formal, o sea, aprobado, documentado y divulgado en la organización, lo que conlleva que no se tienen una estrategia propia para el riesgos, en contraste a la encuestas anterior.

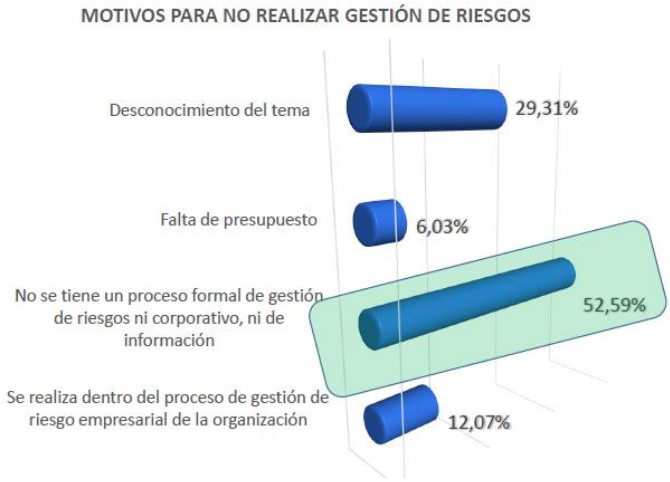

Figura 3: Encuesta sobre motivos para no realizar gestión de riesgos
Asociación Colombiana de Ingenieros de Sistemas – ACIS. 2013. Tomado de http://www.acis.org.co/index.php?id=332

La información entonces se vería seriamente comprometida, al no tener un mecanismo formar o estándar para identificar las diferentes amenazas y ataques a que se ve expuesta, por lo que es necesario un sistema de seguridad que valide, verifique y gestione la protección propia de la información.

De igual manera preocupa que el 29.31% de las empresas encuestadas desconocen el tema de la gestión de riesgo, surge entonces la pregunta, ¿Cómo administran las decisiones y eventos inesperados?

Pero más allá de cómo se mueven los sectores productivos, la legislación en Colombia frente a las telecomunicaciones es muy clara, y ha realizado una serie de exigencias al sector sobre el cumplimiento de temas de seguridad, entre ellos:

- *La resolución número 3066 de la comisión de regulación de comunicaciones de Colombia CRC-3066 del 2011 que indica, entre otras[3]:*
  - *Numeral 11.3[4]: "Informar al usuario en el momento de la celebración del contrato y durante su ejecución, los riesgos relativos a la seguridad de la red y del servicio contratado, los cuales vayan más allá de los mecanismos de seguridad que ha implementado el proveedor para evitar su ocurrencia y sobre las acciones a cargo de los usuarios para preservar la seguridad de la red y de las comunicaciones"*
  - *Artículo 19: Inviolabilidad de las comunicaciones. "Los proveedores de servicios de comunicaciones deben asegurar el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y la prestación de los servicios de seguridad de la información (autenticación, autorización y no repudio), requeridos para garantizar la inviolabilidad de las comunicaciones, de la información que se curse a través de ellas y de los datos personales del usuario en lo referente a la red y servicios suministrados por dichos proveedores"*
- *La ley 1581 de 2012, sobre la protección de datos personales o Habeas Data.*
- *Ley 679 de 2001, sobre pornografía infantil y su decreto reglamentario No. 1524 de 2002,dentro de éste en especial[5]:*
  - *Artículo 6°. Medidas Técnicas. (…)*

    1. Los ISP, proveedores de servicio de alojamiento o usuarios corporativos deberán implementar sistemas internos de seguridad para su red, encaminados a evitar el acceso no autorizado a su red, la realización de spamming, o que desde sistemas públicos se tenga acceso a su red, con el fin de difundir en ella contenido relacionado con pornografía infantil.

    2. Los ISP deben implementar en su propia infraestructura, técnicas de control, basadas en la clasificación de contenidos que tengan como objetivo fundamental evitar el acceso a sitios con contenidos de pornografía infantil.

[3] Resolución 3066 de la comisión de regulación de comunicaciones, consulta en línea en http://www.crcom.gov.co/index.php?idcategoria=61450

[5] Tomado textual de la ley Colombiana, consulta en línea en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5551

> *La clasificación de estos contenidos se sujetará a la que efectúen las diferentes entidades especializadas en la materia. Dichas entidades serán avaladas de manera concertada por el Ministerio de Comunicaciones y el Instituto Colombiano de Bienestar Familiar-ICBF.*
>
> *3. Los prestadores de servicios de alojamiento podrán utilizar herramientas tecnológicas de monitoreo y control sobre contenidos alojados en sitios con acceso al público en general que se encuentran en su propia infraestructura.*
>
> *4. Los ISP y proveedores de servicios de alojamiento deberán ofrecer o informar a sus usuarios, sobre la existencia de mecanismos de filtrado que puedan ser instalados en los equipos de estos, con el fin de prevenir y contrarrestar el acceso de menores de edad a la pornografía.*
>
> *Así mismo los ISP deberán facilitar al usuario el acceso a la información de criterios de clasificación, los valores y principios que los sustentan, la configuración de los sistemas de selección de contenido y la forma como estos se activan en los equipos del usuario.*
>
> *5. Cuando una dirección es bloqueada por el ISP, se debe indicar que esta no es accesible debido a un bloqueo efectuado por una herramienta de selección de contenido.*
>
> *6. Los ISP y proveedores de servicios de alojamiento deberán incluir en sus sitios, información expresa sobre la existencia y los alcances de la Ley 679 de 2001, y sus decretos reglamentarios.*
>
> *7. Los ISP y proveedores de servicios de alojamiento deberán implementar vínculos o "links" claramente visibles en su propio sitio, con el fin de que el usuario pueda denunciar ante las autoridades competentes sitios en la red con presencia de contenidos de pornografía infantil*

Como se ve, las empresas de telecomunicaciones tienen la responsabilidad (por convicción y obligación) a fortalecer sus mecanismos de protección, que les permita dar garantía y confianza al cliente, proveedores y accionistas sobre su objeto de negocio, se hace necesario entonces, como una buena propuesta, fomentar la planeación, diseño e implementación de un sistema de gestión de seguridad de la información – SGSI, que logre cubrir todos los aspectos sobre la protección propia de la información, en especial, en los diferentes sistemas de información donde haya procesamiento automático de ésta (Sistemas de Información).

3. Definición del alcance

El sistema de Gestión de Seguridad de la Información – SGSI comprende los sistemas de información que apoyan a los procesos para la operación de Telecomunicaciones: Gestión logística, Ventas y PRQ, Gestión del servicio y la operación, Gestión de la relación con proveedores, Gestión de inventario y gestión de la facturación y el recaudo, dichos procesos son apoyados por los sistemas de información CRM, OSM, Facturación y portal Web para el comercio electrónico, así mismo el SGSI también comprenderá el proceso financiero y su sistema de información ERP.

Éste alcance está delimitado por la declaración de aplicabilidad y la implementación de controles se limita por el posible presupuesto aprobado.

4. Objetivos del plan director

Los siguientes son los objetivos del plan director:

a) *Buscar el apoyo, dirección y aprobación de manera continua del SGSI en la alta gerencia y hacia las partes interesadas sobre el alcance definido.*
b) *Identificar, calificar y hacer un tratamiento adecuado de los riesgos que puedan impactar negativamente la información, los procesos y la organización sobre las redes de telecomunicaciones y los servicios asociados al segmento de hogares, implementando las salvaguardas que permitan reducir el nivel de exposición frente a ataques informáticos.*
c) *Buscar que la información sobre las redes de telecomunicaciones este protegida contra ataques informáticos y maliciosos en general e implementar los controles que eviten modificaciones no autorizadas.*
d) *Entregar valor y confianza a los clientes de hogares a través del mejoramiento continuo en seguridad en las redes de telecomunicaciones.*
e) *Dar cumplimiento a la normatividad y legislación vigente en el sector de las comunicaciones acorde a su aplicabilidad.*
f) *Fomentar la cultura organizacional, la capacitación y toma de conciencia frente a los riesgos asociados a la información sobre las redes.*

5. Análisis

Para el análisis se hará una breve descripción de la norma ISO/IEC 27001:2005 y sus mejoras, además, del análisis diferencial.

a. La norma ISO/IEC 27001

La norma ISO/IEC 27001 es reconocida como una de las mejores prácticas empresariales a nivel de seguridad de la información, que basada en la gestión del riesgo se establece para crear, operar, revisar, mantener y mejorar de la seguridad de la información a través de un sistema de gestión de seguridad.

Lo que se espera de un SGSI es que sea concordante con las necesidades de la organización y los objetivos del negocio, con ello, poder generar el valor que las partes interesadas requieren. Bajo su enfoque en procesos, el SGSI está basado en el ciclo de Deming:

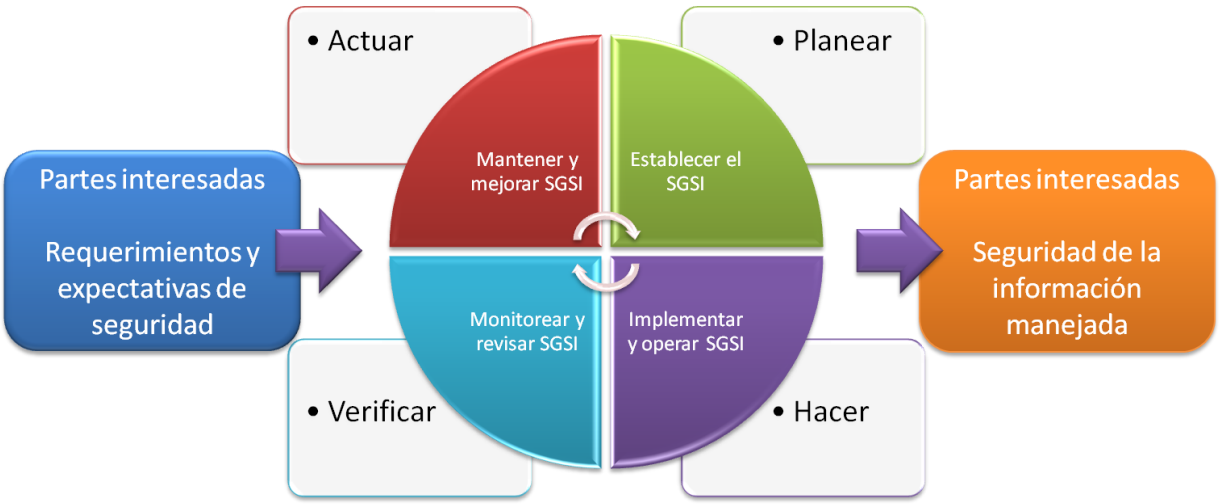

Figura 4: Ciclo de Deming - PHVA

Como elemento resumen, la norma ISO/IEC 27001:2005 tiene 11 dominios, 38 objetivos de control y 133 controles, de los cuales se deben seleccionar aquellos que deben ser implementados acorde al alcance.

Por otro lado, la ISO 27002 ha evolucionado considerablemente[6]*, desde el código de buenas prácticas (Estándar Ingles) BS 7799 parte 1 del el año 1995, evolucionando en el año 1998 a la parte 2, en la cual se hace la primera aproximación a las especificaciones de un SGSI, luego, la ISO adopta ambas partes y genera el estándar ISO/IEC 17799 en el año 2000 y en el año 2005 sale la revisión mejorada de la 17799 en conjunto con la ISO/IEC 27001, quedando la primera como un anexo de la segunda.*

El 25 de septiembre de 2013, se apruebas nuevas versiones de las normas ISO/IEC 27001:2013 e ISO/IEC 27002

En los nuevos ajustes en la versión ISO/IEC 27001:2013 el más importante es una adecuación a una estructura de alto nivel, con ello, es más fácil y simple la implementación y homologación con otras normas enfocadas a sistemas de gestión, quedando un tiempo de transición de la versión 2005 a la nueva, que puede ser de 2 años aproximadamente (luego de esto, se retirará la versión 2005), así mismo, las acciones preventivas hacen parte de la gestión de riesgos.

Para la nueva versión de la ISO/IEC 27002:2013 se encuentra una reorganización de dominios, se crean unos y se retiran otros. De 11 dominios se aumentan a 14 y ha disminuido el número de controles, de 133 a 113.

[6] Tomado y ajustado de http://www.iso27000.es/iso27000.html

Se crean los dominios de criptografía y relación con proveedores, el dominio "Gestión de las comunicaciones y operación" fue separado en 2, quedando la lista así[7]*:*

- 5 Security Policies
- 6 Organization of information security
- 7 Human resource security
- 8 Asset management
- 9 Access control
- 10 Cryptography
- 11 Physical and environmental security
- 12 Operations security
- 13 Communications security
- 14 System acquisition, development and maintenance
- 15 Supplier relationships
- 16 Information security incident management
- 17 Information security aspects of business continuity
- 18 Compliance

La nueva norma trae entonces, mucho más claridad para el entendimiento de los controles a implementar y se ajustan algunos controles que estaban inmersos en otros y que seguramente no tenían una relación clara.

b. Análisis diferencial

Para el análisis diferencial (Anexo 1), se realizó un nivel de medición que sirve como referencia, no necesariamente se encasilla sobre el valor (se puede dar un valor porcentual diferentes), es solo para tener un nivel y estado de la implementación.

Porcentaje de implementación	*Descripción del porcentaje*
0%	*No se tiene implementación*
25%	*Se ha iniciado la implementación o está en etapa de planeación*
50%	*Esta implementado, pero no se ha aprobado ni divulgado.*
100%	*Esta implementado, aprobado y divulgado, además se monitorea.*

Tabla 1: Tabla medición de controles - Análisis diferencial

Así mismo, la fuente de información de la norma se obtuvo desde el blog de Javier Cao Avellaneda en la URL http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html, allí se pueden obtener las normas ISO 27001 e ISO 27002 para efectos académicos.

[7] Lista tomada textualmente de http://blog.segu-info.com.ar/2013/02/cambios-nueva-iso-27001-2013-III.html#ixzz2KtZbBL6V

En el anexo 1 se entrega la forma como se calificaron cada uno de los ítems de la norma, como resultado de la evaluación se obtuvo las siguientes gráficas para las 2 normas:

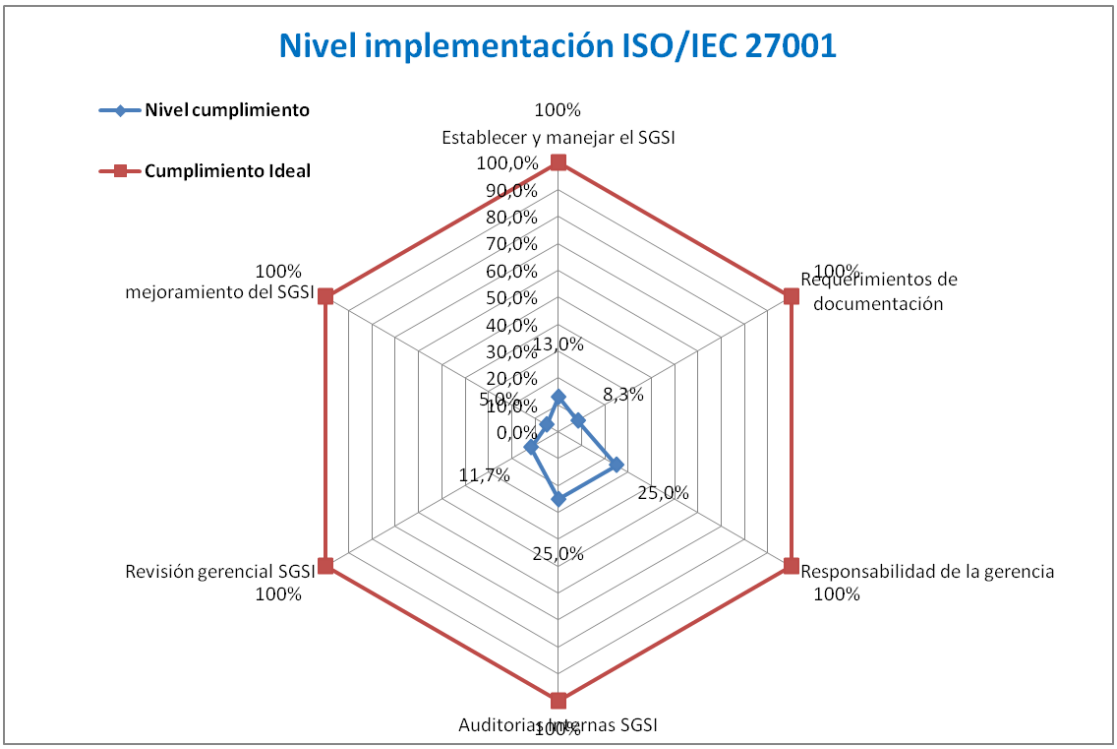

Figura 5: Nivel de implementación ISO 27001

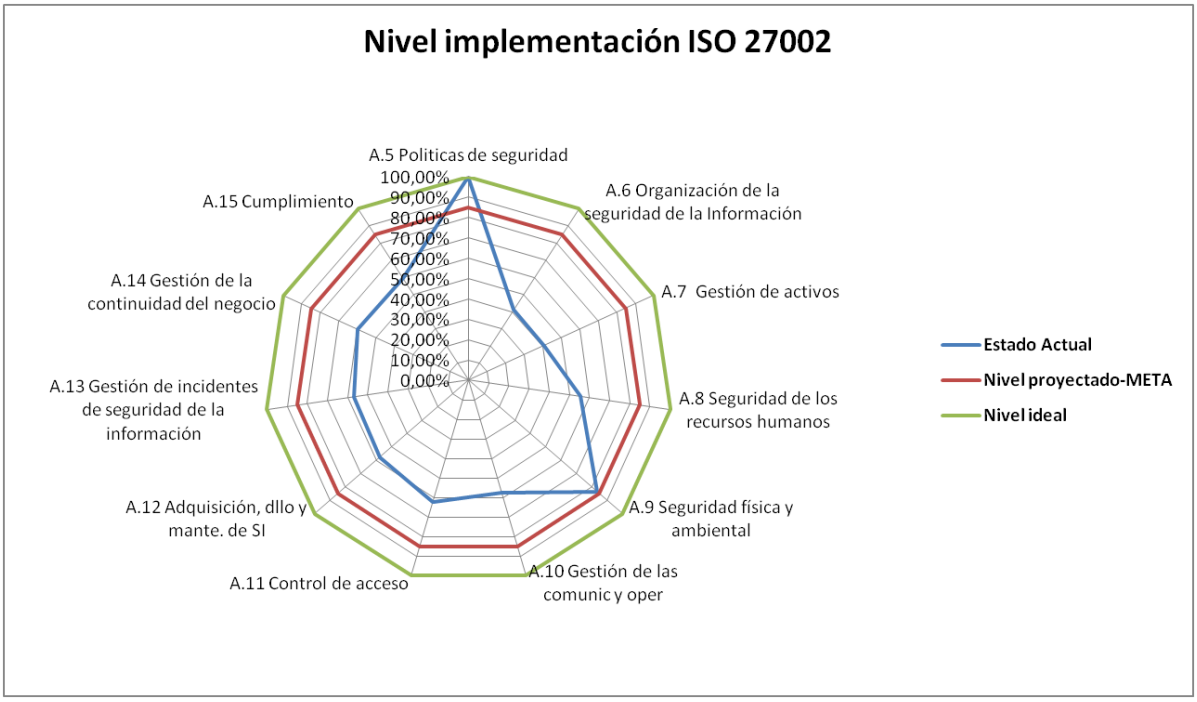

Figura 6: Nivel de implementación ISO 27002

6. Políticas de seguridad

La política de seguridad es una declaración ética, responsables y de estricto cumplimiento en toda la organización, la cual es desplegada a través de las diferentes guías y procedimientos, procurando que los riesgos sean tratados adecuadamente.

El objetivo de la política de seguridad es entender que la información en toda la organización debe ser protegida, manteniendo los niveles óptimos de seguridad, permitiendo velar porque dicha información (sea propia y/o de terceros) se le conserve la confidencialidad, integridad y disponibilidad.

En el anexo 2 podemos encontrar el documento de política de seguridad.

7. Plan de auditoria

El siguiente plan de auditoría enmarca los elementos necesarios para el SGSI, dicho plan se desarrolla por etapas de ejecución, así mismo, en el anexo 3 se encuentra el formato informe a entregar.

a. Objetivos

Ejecutar el plan de auditoría para la planeación de un SGSI, así como la auditoria para la implementación de algunos controles para la empresa.

b. Planeación

i. Alcance

- *El plan de auditoría se limita a la planeación del SGSI y a la implementación de algunos controles sobre el alcance definido.*
- *Auditoria técnica (black-box y White-box) sobre algunos elementos tecnológicos en las redes de telecomunicaciones, bases de datos y aplicaciones.*

ii. Cronograma

En el anexo 4, se puede consultar el detalle del cronograma

iii. Procedimiento de auditoria

El siguiente diagrama representa la ejecución del plan:

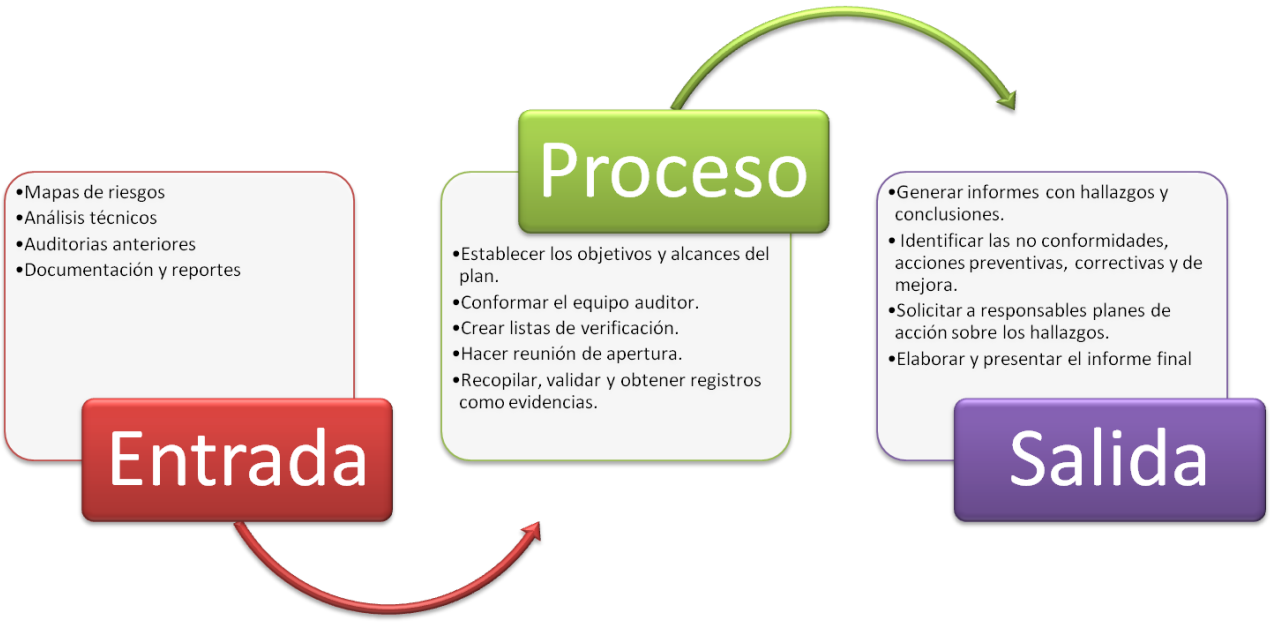

Figura 7: Proceso general de auditoria

iv. Dimensionamiento de recursos

Se define el siguiente esquema de trabajo:

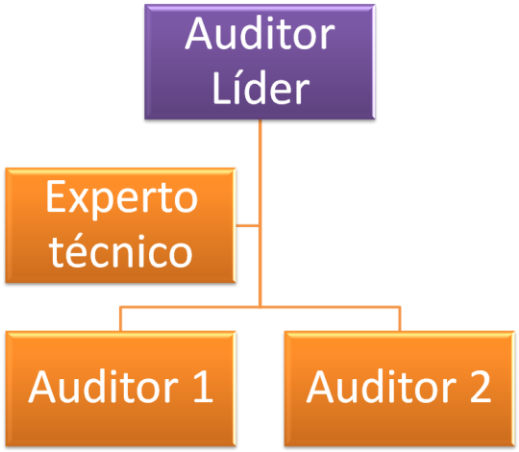

Figura 8: Estructura del equipo de auditoria

Auditor líder:

Profesión – perfil académico	Ingeniería de Sistemas, ingeniería informática, ingeniería de computación, ingeniería telemática, de telecomunicaciones o afines.
Estudios	Especialista, postgrado o maestría en administración, gestión de proyectos, gerencia o afines.
Cargo	Auditor Líder
Número de personas a cargo	3
Experiencia	Más de 3 años en gestión, administración y liderazgo de proyectos de auditoría en sistemas de gestión de seguridad -SGSI
Funciones principales	• Responsable de definir, diseñar, ejecutar y hacer seguimiento al plan de auditoría. • Generar reportes periódicos a la alta gerencia y dueños del proyecto. • Gestionar al personal a cargo. • Revisar y avalar los entregables y documentos generados por los auditores. • Ejecutar y controlar el presupuesto asignado. • Actuar con ética, responsabilidad e independencia frente a la ejecución de la auditoria
Conocimientos complementarios	Manejo de Office, gestión de proyectos, proyecciones financieras Preferiblemente, estar certificado como auditor líder en ISO 27001.
Competencias	Buenas relaciones personales, manejo de público, actuar con ética, responsabilidad e independencia frente a la ejecución de la auditoria

Experto técnico:

Profesión – perfil	Ingeniería de Sistemas, ingeniería informática, ingeniería de computación,

académico	ingeniería telemática, de telecomunicaciones o afines.
Estudios	Especialista, postgrado o maestría en seguridad, redes, informática o afines.
Cargo	Experto técnico
Número de personas a cargo	0
Experiencia	Más de 3 años en desarrollo de pruebas técnicas (ethical hacking).
Funciones principales	• Ejecutar auditorias técnicas sobre los sistemas y plataformas tecnológicas. • Generar reportes técnicos sobre los hallazgos. • Actuar con ética, responsabilidad y confidencialidad en la ejecución de las pruebas técnicas. • Coordinar otras personas que apoyen esta tarea.
Conocimientos complementarios	Estar certificado en algunas de los siguientes temas o similares: • Ethical Hacker certified • Certified Security Analyst • Computer Hacking Forensic Investigator • Chief Information Security Officer • Certified Cyber Forensics Professional • Penetration Tester
Competencias	Buenas relaciones personales, actuar con ética y confidencialidad, responsabilidad e independencia frente a la ejecución de la auditoria

Auditores 1 y 2*:*

Profesión – perfil académico	Ingeniería de Sistemas, ingeniería informática, ingeniería de computación, ingeniería telemática, de telecomunicaciones o afines.
Estudios	Especialista, postgrado o maestría en seguridad, redes, informática o afines.
Cargo	Profesional en auditoria
Número de personas a cargo	0
Experiencia	Más de 2 años en desarrollo de auditorías a sistemas de información y tecnologías en general.
Funciones principales	• Analizar, diseñar, construir, probar, entrenar, verificar y controlar la ejecución de los planes de auditoría. • Debe tener conocimientos sobre arquitectura de aplicaciones y gestión de base de datos, administración de sistemas Linux y servidores Web, gestión de repositorio de datos • Realizar entrevistas al personal • Obtener evidencias de las implementaciones • Generar reportes de hallazgos y entregar informes periódicos al auditor líder. • Ejecutar actividades propias del cargo
Conocimientos complementarios	Manejo de Office, gestión de proyectos, proyecciones financieras Experiencia o estar capacitado como auditor líder en ISO 27001.
Competencias	Buenas relaciones personales, actuar con ética y confidencialidad, responsabilidad e independencia frente a la ejecución de la auditoria Capacidad de trabajar en equipo para conseguir metas cortas de una

	manera muy eficiente y rápida, con la visión de trabajo para un proyecto en permanente desarrollo.

v. Plan de auditoria

Entradas:

- *Se debe obtener los informes de riesgos anteriores y con base en estos revisar/validar como se ha realizado el tratamiento.*
- *Recopilar todos los análisis técnicos: Informes forense, ethical hacking, análisis de vulnerabilidades/pruebas de intrusión.*
- *Validar las auditorias anteriores, revisando el estado de los hallazgos y el nivel de cumplimiento de las acciones de mejora.*
- *Identificar las fuentes de documentación de reportes que aporten evidencia.*

Proceso:

- *Se debe definir claramente el objetivo y alcance de la auditoria, así mismo, conformar el equipo de trabajo.*
- *Se debe definir el tipo de auditoría técnica a realizar, para nuestro caso, se realizarán Black-Box o pruebas de caja negra y White-box o pruebas de caja blanca.*

Salidas:

- *Elaborar los informes de auditoría acorde al formato "Informes finales de auditoría" localizado en el anexo 3.*

8. Indicadores

El numeral 4.2 de la norma ISO/IEC 27001 indica la necesidad de definir e implementar mediciones de la efectividad de los controles, para ello se han definido los siguientes 10 indicadores[8] que pueden ser revisamos en el anexo 5:

Número del indicador	Nombre
1.	*Nivel de implementación del SGSI – ISO 27002*
2.	*Compromiso de la alta dirección*
3.	*Incidentes de seguridad*
4.	*Gestión de riesgos*
5.	*Capacitación, entrenamiento y toma de conciencia*
6.	*Seguridad física y ambiental*
7.	*Control de acceso*
8.	*Controles criptográficos*
9.	*Protección contra software malicioso*
10.	*Análisis de vulnerabilidades*

Tabla 2: Lista de indicadores

El procedimiento para medir los indicadores es:

a) *Buscar fuentes o posibles fuentes como análisis de riesgos, controles implementados, informes de auditorías, análisis de vulnerabilidades, entre otros.*
b) *Tabular cada informe validando a qué control o controles posibles apoya.*
c) *Se valida /define la escala de calificación para cada control o grupo de controles.*
d) *Se da una calificación conforme a las fuentes y evidencias encontradas.*
e) *Se validan los % de cumplimiento acorde a los compromisos con la alta dirección.*
f) *Se validan las gráficas que de forma automática se obtienen*
g) *Se puede publicar (si así se requiere) los resultados obtenidos. Estos harán parte de la revisión por la dirección.*

9. Procedimiento Revisión por la dirección

La alta dirección como responsable de la aprobación del SGSI, debe realizar de manera anual una revisión al sistema, indicando los asuntos prioritarios de éste y aprobado los ajustes/acciones de mejora que se tengan.

Para ello, se debe convocar al menos 20 días antes de la reunión a la alta gerencia y enviar los informes de gestión para ser revisados, como insumos de ***entrada*** *se deben tener:*

- *Los indicadores (y sus medidas de la efectividad) y revisiones gerenciales previas.*
- *Resultados de las auditorias.*

[8] La definición de la tabla de indicadores fue obtenido de la ISO/IEC 27004 y la norma NIST 800-55.

- *Revisión y estado de las políticas de seguridad.*
- *Estado de la gestión de riesgos e incidentes de seguridad.*
- *Nuevos requerimientos del SGSI, así como mecanismos para el mejoramiento del desempeño y la efectividad.*
- *Retroalimentaciones de las partes interesadas y recomendaciones de mejoramiento.*
- *Estado de las acciones correctivas, preventivas y de mejora.*
- *Resultados de riesgos: Riesgos no tratados o resultado de los que no tuvieron la efectividad esperada.*

Para la presentación de la información, es necesario llevarla en el formato del anexo 6: "Presentación revisión por la dirección".

Culminada la reunión se debe generar un acta de comité con las respectivas conclusiones y decisiones, en el anexo 7 podemos encontrar el formato para ello.

10. Roles y responsabilidades

Para el SGSI se han definido los siguientes roles y responsabilidades:

Nombre del rol	*Funciones / Responsabilidades*
Alta dirección	▪ Aprobar los recursos financieros y humanos para el SGSI ▪ Aprobar y firmar las políticas de seguridad y sus actualizaciones. ▪ Aprobar en última instancia el SGSI y los procedimientos respectivos. ▪ Gestionar adecuadamente los riesgos de alto nivel que se hayan detectado. ▪ Revisar y ajustar los indicadores de su competencia. ▪ Aprobar los planes de continuidad de negocio. ▪ Participar activamente de las reuniones programadas.

Comité de seguridad	▪ Revisar, mantener y aprobar en primera instancia el SGSI.
	▪ Revisar, gestionar y aprobar los planes de seguridad e implementaciones de controles.
	▪ Hacer seguimiento al cumplimiento de las políticas de seguridad.
	▪ Gestionar las mediciones de los indicadores y presentarlos a las partes interesadas.
	▪ Gestionar las acciones preventivas, correctivas y de mejora que surgen durante las revisiones periódicas.
	▪ Gestionar adecuadamente los incidentes de seguridad y la continuidad del negocio.
	▪ Participar activamente de las reuniones programadas.
	▪ Hacer parte del comité las siguientes áreas/personas:
	  ▪ Gerente de Tecnología
	  ▪ Gerente de recursos humanos
	  ▪ Área de seguridad física
	  ▪ Otras áreas de apoyo.

Área de seguridad	▪ Liderar la implementación y mantenimiento del SGSI.

	▪ Liderar las reuniones del comité de seguridad. ▪ Participar de las capacitaciones programadas. ▪ Verificar los informes de la auditoria. ▪ Crear, ajustar e implementar los planes de toma de conciencia y capacitación sobre seguridad. ▪ Utilizar todos los medios técnicos y profesionales a su alcance para implementar y mantener el SGSI. ▪ Realizar análisis de riesgos de seguridad de la información. ▪ Gestionar, realizar y/o liderar pruebas de instrucción y Ethical hacking.
Área de auditoria	▪ Llevar a cabo las auditorias del SGSI de manera periódica. ▪ Generar las respectivas acciones preventivas, correctivas y de mejora sobre el sistema. ▪ Convocar a las reuniones/comités de seguimientos. ▪ Liderar los planes de auditoría, retroalimentando al comité de seguridad. ▪ Ejecutar las acciones con ética, respeto, transparencia, independencia e imparcialidad.
Áreas de operación y desarrollo	▪ Implementar los controles de seguridad seleccionados. ▪ Utilizar todos los medios técnicos y profesionales a su alcance para operar el SGSI. ▪ Participar de las capacitaciones programadas. ▪ Verificar el nivel de cumplimiento de la implementación de los controles. ▪ Analizar e implementar los hallazgos de los planes de auditoría.
Áreas de apoyo	▪ Participar del SGSI cuando sean convocados. ▪ Analizar e implementar los hallazgos de los planes de auditoría que estén a su alcance.
Líder o responsable de seguridad	▪ Coordinar el equipo de trabajo (equipo de seguridad). ▪ Gestionar la obtención de entradas para los indicadores, mapas de riesgos y demás informes. ▪ Recibir y asignar funciones y tareas a los miembros del equipo de seguridad. ▪ Coordinar y gestionar las capacitaciones en seguridad. ▪ Obtener el presupuesto ▪ Gestionar elementos contractuales y con proveedores.
Administrador técnico de seguridad	▪ Administrar las plataformas de seguridad como Firewall y el anti-virus ▪ Obtener y analizar reportes de seguridad ▪ Coordinar el monitoreo de eventos de seguridad. ▪ Administrar/gestionar el control de acceso a las redes y aplicativos.
Administrador de redes y plataformas	▪ Implementar mecanismos de seguridad sobre redes y plataformas. ▪ Entregar insumos para los reportes y monitoreos de seguridad. ▪ Cumplir y hacer cumplir las políticas de seguridad frente al control de acceso a las redes. ▪ Apoyar el diseño de mecanismos de control sobre las redes.
Abogado	▪ Apoyar la redacción y revisión de los contratos con proveedores. ▪ Revisar el estado de los contratos de trabajo. ▪ Ejecutar los procesos administrativos y/o disciplinarios. ▪ Revisar periódicamente la legislación vigente.
Analista de comunicación y diseñador gráfico	▪ Apoyar con estrategias comunicacionales y de cultura para la implementación y gestión del SGSI. ▪ Construir piezas publicitarias para la sensibilización y planes de cultura.

	▪ Diseñar elementos de merchandansing que se apropien de la estrategia de seguridad. ▪ Apoyar la implementación de los planes de cultura y sensibilización.

Tabla 3: Roles y responsabilidades del SGSI

11. Metodología para el análisis y evaluación de riesgos

La metodología para la gestión de riesgos a utilizar es la ISO/IEC 31000 la cual contiene los siguientes componentes[9]:

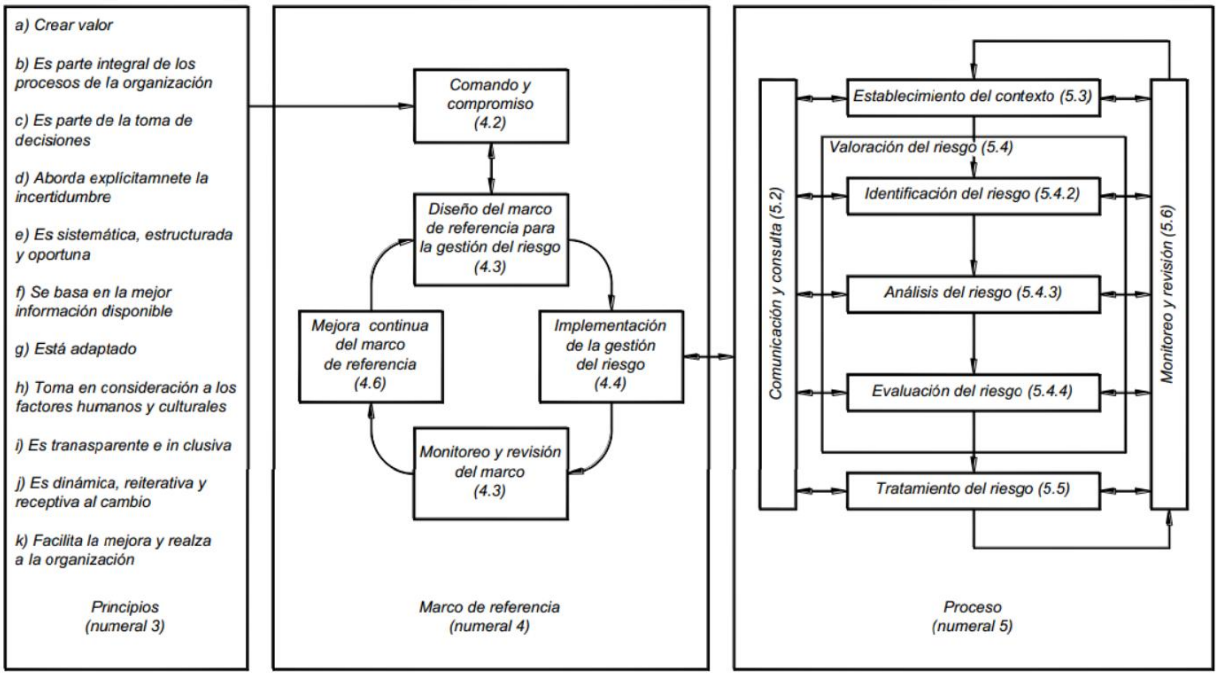

Figura 9: NTC-ISO 31000, norma técnica de gestión de riesgo

Esta norma las directrices necesarias para una adecuada gestión de gestión del riesgo y puede ser aplicada a cualquier tipo de organización (independiente de su naturaleza jurídica), para nuestro caso particular, se hará una aplicabilidad sobre el alcance definido en el proyecto, en especial, a las tecnologías de información y comunicaciones.

La norma ISO 31000 derivada de la AS/NZS 4360:2004, se constituye como una metodología imprescindible para la gestión del riesgo empresarial, y es aplicable a cualquier industria independiente de su objeto social.

[9] Copia textual de http://tienda.icontec.org/brief/NTC-ISO31000.pdf

A continuación se ilustra en qué consiste cada uno de los pasos de la ISO 31000, así mismo, para una mejor calificación del riesgo, en el anexo 8 podemos encontrar una matriz en Excel que nos ayudara a calificar los riesgos.

a) Comunicación y consulta.

Desarrolla el plan de comunicación para las partes interesadas (internas y externas), en dicho plan se convoca/reúne a las diferentes áreas que puedan tener conocimiento sobre el alcance definido, así mismo, se define los mecanismos de comunicación tales como:

- *Cantidad de reuniones por semana y duración de éstas.*
- *Medios de comunicación: Correo, chat, teleconferencias, video conferencias, presencial.*
- *Quién será el equipo de trabajo que estará al frente del análisis de riesgos y cuáles serán las áreas de apoyo a las que se deba convocar.*

Ésta fase fortalece la comunicación efectiva y eficaz con las diferentes áreas y personas, con ello, tener información más fiable a la hora de definir el contexto y hacer la calificación respectiva del riesgo.

a) Establecimiento del contexto

Ésta es una de las etapas fundamentales en la gestión del riesgo, dado que nos dará el límite de los objetivos dentro de la organización. Si no se establece claramente el contexto y/o el ámbito de aplicación, es posible de los resultados finales no cuenten con la veracidad que se requiere para el sistema de referencia, con ello, podría darse pérdida de tiempo y credibilidad, al realizar un esfuerzo grande donde las otras áreas y la misma gerencia estén esperando algo diferente.

El contexto puede definirse desde 2 puntos de vista:

1. **Desde lo externo**

   Dentro de éste tipo de contexto está asociado a los eventos que están por fuera de a organización y que eventualmente pueden afectarla, como lo político, urbano, social, financiero/económico, ámbito local, regional o internacional.

   También, terceras partes que tengan asociación con la empresa como la Junta directiva, proveedores y la misma competencia.

2. **Desde lo Interno**

Dentro del contexto interno se pueden identificar los diferentes procesos o tecnología que apoyan el negocio y se limita a los objetivos propios de la organización o a las funciones especiales de un área, proceso, procedimiento o tecnología.

Para la selección de este tipo de contexto, es necesario conocer y reconocer los procesos internos, la cultura organizacional, la tecnología que soporta los proyectos/procesos, la documentación y lineamientos organizacionales, los sistemas de información y aplicaciones, las relaciones contractuales, entre otros.

Una de las estrategias para la definición del alcance puede ser, partiendo del objetivo del análisis de riesgos, limitarlo a algo que sea alcanzable en el tiempo y recursos.

Para el caso particular de éste proyecto, el alcance estará asociado al SGSI propiamente.

b) Identificación del riesgo

En esta etapa se debe identificar los activos de información y las diferentes amenazas.

1) Levantamiento de activos

Éste es un paso fundamental, dado que los riegos aplican sobre los activos, es por ello la necesidad de de ser muy precisos en éste levantamiento. Es necesario categorizar entre activos tangibles e intangibles.

Una buena fuente de activos de información se puede obtener desde la metodología MAGERIT[10] y su catalogo de activos- amenazas. En esta etapa se debe hacer el levantamiento de las amenazas y vulnerabilidades que pueden tener/afectar los diferentes activos o grupos de activos, de esta forma, se comprende mejor el riesgo, además, se deben agrupar por factores de riesgos.

2) Factores de riesgos y amenazas

Un factor de riesgo es una agrupación de eventos o situaciones que tiene similares características y que pueden ser agrupadas para un mejor entendimiento y control.

Algunos factores de riesgos son:

- *Amenazas TIC – de Tecnologías de información y comunicaciones*
- *Amenazas Naturales*
- *Amenazas sociales o humanas*

[10] https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_II_catalogo.pdf

- *Amenazas administrativas o estratégicas*

AMENAZAS TIC	AMENAZAS NATURALES	AMENAZAS HUMANAS/SOCIALES	AMENAZAS ESTRATÉGICAS Y ADMINISTRATIVAS

Tabla 4: Ejemplo de listado de amenazas

Para lo cual deberíamos razonar sobre lo siguiente[11]*:*

- *¿Qué puede suceder, dónde y cuándo?*

De acá deberíamos analizar las diferentes fuentes de riesgos como las listas de distribución, páginas de proveedores, NVD (national vulnerabilities database), foros y estados del arte en temas de seguridad.

- *¿Por qué y cómo puede suceder?*

Acá debemos obtener las diferentes causas (vulnerabilidades) de por qué y cómo puede suceder el riesgos, así mismo, los posibles agentes generadores del riesgos, lo que nos permitirá más adelante establecer diferentes mecanismos de protección que ayuden a reducir la probabilidad y/o el impacto.

- *¿Qué herramientas técnicas nos puede ayudar a obtener el inventario de amenazas/vulnerabilidades?*

Podemos apoyarnos de herramientas técnicas para conocer posibles amenazas o vulnerabilidades, así como análisis anteriores que nos permita conocer exposiciones al riesgo. Las herramientas técnicas son una fuente importante desde lo técnico, para conocer nuestros sistemas de información y plataformas tecnológicas.

Así mismo, en esta categoría podemos utilizar juicios de los expertos y lluvias de ideas.

c) Análisis del riesgo

Analizar los riesgos implica comprender más acertadamente los riesgos, considerando las causas y efectos si éstos se consolidan. En ésta etapa se debe realizar lo siguiente:

[11] Tomado y ajustado de http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf

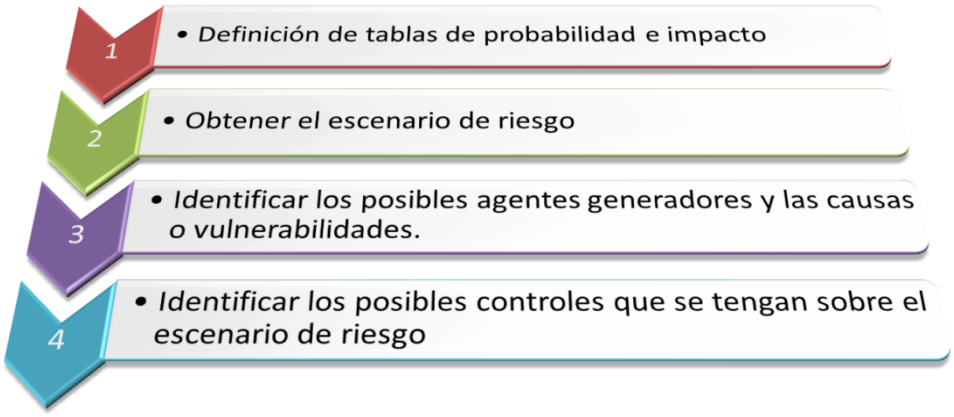

Figura 10: Etapa análisis de riesgos

1. *Definición de las tablas de probabilidad e impacto, la cual llevaremos a una matriz de 5x5 que nos dará un nivel más acertado del riesgo. Así mismo, se obtendrás*

Para esto, se han definido las siguientes tablas de probabilidad e impacto:

Para la probabilidad:

Nivel	Rangos	Descripción
1	**Raro**	*Puede ocurrir solo bajo circunstancias excepcionales*
2	**Improbable**	*Podría ocurrir algunas veces*
3	**Posible**	*Puede ocurrir en algún momento*
4	**Probable**	*Probabilidad de ocurrencia en la mayoría de las circunstancias*
5	**Casi cierto**	*La expectativa de ocurrencia se da en la mayoría de circunstancias*

Tabla 5: Definición de tablas de probabilidad

Para el impacto, es necesario identificar qué factor de impacto se va a analizar, algunos de los factores de impacto son:

- *Daño a la imagen*
- *Pérdidas económicas*
- *Impacto en clientes/mercado.*
- *Pérdida de la operación / información*

Para nuestro caso, se evaluará los riesgos en términos de pérdida de operación / información, bajo la siguiente tabla:

Impacto en la OPERACIÓN/INFORMACIÓN		
Nivel	**Rangos**	**Descripción**
1	**Insignificante**	*Hay una afectación en la operación menor a 4 y la puede resolver la mesa de ayuda.*
2	**Menor**	*Hay una afectación en la operación entre 4 y 12 horas, es necesario escalarlo a un*

		segundo nivel
3	**Moderado**	*Hay una afectación en la operación/información entre 12 y 36 horas, se requiere consulta el proveedor dueño de la plataforma. Es manejable la pérdida de información, se puede recuperar.*
4	**Mayor**	*Hay una afectación en la operación/información entre 36 y 72 horas, se requiere al proveedor en sitio. Puede haber pérdida importante de información*
5	**Catastrófico**	*Hay una afectación en la operación/información por más de 72 horas, es necesario establecer un mecanismo de procesamiento alterno. Podría haber sanciones o multas*

Tabla 6: Definición de tablas de impacto

2. *Para la obtención de los escenarios de riesgos, se debe realizar el cruce de amenazas/ataques con respecto a la afectación sobre los activos de información.*

	A	B	C	D	E	F	G
1	**AMENAZAS/ACTIVOS**	Activo 1	Activo 2	Activo 3	Activo 4		
2	Amenaza 1	x		x			
3	Amenaza 2		x				
4	Amenaza 3	x	x		x		
5	Amenaza 4				x		
6	Amenaza 5	x		x			
7	Amenaza 6			x			
8							

Figura 11: Ejemplo de Obtención del escenario de riesgo

Esto es, como las diferentes amenazas actúan o afectan en los diferentes activos de manera directa, se debe fijar un "x" cuando una amenaza pueda afectar a uno o varios activos.

3. *Luego del cruce de escenario, éstos se llevan al listado de riesgos acorde a la afectación de las amenazas sobre los activos y desde éste listado, se debe generar los posibles agentes generadores de esos riesgos, esto es, entes externos al sistema con potencial daño, así como las posibles causas o vulnerabilidades que puedan estar en los activos. Eso nos permitirá en los planes de tratamiento, conocer como poder reducir la probabilidad y/o el impacto.*

El archivo Excel de apoyo, traerá los escenarios de riesgos los cuales serán conformados por las amenazas vs. Activos seleccionados con "x".

	A	B	C	D
1		Traer Escenarios		
2	**Escenario del riesgos**	**Agente Generador**	**Causa**	**Controles actuales**
3	Amenaza 1 -- Activo 1			
4	Amenaza 1 -- Activo 3			
5	Amenaza 2 -- Activo 2			
6	Amenaza 3 -- Activo 1			
7	Amenaza 3 -- Activo 2			
8	Amenaza 3 -- Activo 4			
9	Amenaza 4 -- Activo 4			
10	Amenaza 5 -- Activo 1			
11	Amenaza 5 -- Activo 3			
12	Amenaza 6 -- Activo 3			

Figura 12: Ejemplo de definición de agente generador y causa

4. *Es de suma importancia identificar qué controles actuales se poseen sobre el escenario de riesgos, dado que esto, no podría reducir los posibles impactos a la hora de calificar/evaluar.*

d) Evaluación del riesgo

Para esta fase se debe realizar lo siguiente:

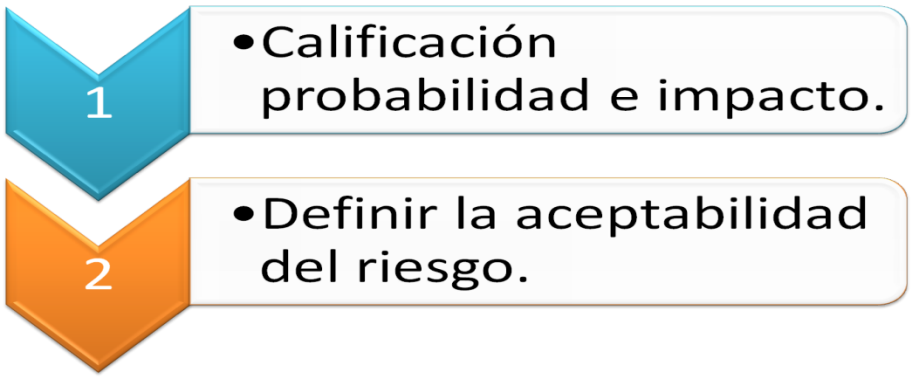

Figura 13: Pasos para la evaluación del riesgo

1. *En la calificación de los riesgos, se debe seleccionar por cada escenario de riesgo su probabilidad de ocurrencia (tabla 5) y en su impacto (tabla 6), con ello, establecer el nivel de riesgos*
    a. *Nivel de riesgo = Probabilidad x Impacto*

Para la valoración de es necesario tener en cuenta qué controles se tienen al respecto (controles actuales) los cuales fueron obtenidos en el paso de "análisis de riesgo", dado que estos pueden influenciar positivamente en los niveles de riesgos finales.

Una vez identificadas las tablas, se procese con la valoración de la probabilidad, así mismo, con el impacto.

1	**Calificación con Controles**					
2	**ESCENARIO**	**PROBABILIDAD**		**IMPACTO OPERACIÓN**		**Riesgo Probabilidad*Impacto**
3	*Amenaza 1 -- Activo 1*	*Raro*	*1*	*Insignificante*	*1*	*1*
4	*Amenaza 1 -- Activo 3*	*Improbable*	*2*	*Mayor*	*4*	*8*
5	*Amenaza 2 -- Activo 2*	*Casi seguro*	*5*	*Moderado*	*3*	*15*
6	*Amenaza 3 -- Activo 1*	*Posible*	*3*	*Mayor*	*4*	*12*
7	*Amenaza 3 -- Activo 2*	*Casi seguro*	*5*	*Catastrofico*	*5*	*25*
8	*Amenaza 3 -- Activo 4*	*Casi seguro*	*5*	*Insignificante*	*1*	*5*
9	*Amenaza 4 -- Activo 4*	*Posible*	*3*	*Menor*	*2*	*6*
10	*Amenaza 5 -- Activo 1*	*Improbable*	*2*	*Moderado*	*3*	*6*
11	*Amenaza 5 -- Activo 3*	*Improbable*	*2*	*Menor*	*2*	*4*
12	*Amenaza 6 -- Activo 3*	*Casi seguro*	*5*	*Catastrofico*	*5*	*25*

Figura 14: Ejemplo evaluación del riesgo

2. *Para la aceptabilidad el riesgo, se ha considerado dejar el estándar propuesto quedando así::*

Nivel	*Descripción*
Bajo – B	*Nivel aceptable de riesgo, es susceptible a acciones de mejora*
Moderado – M	*Nivel aceptable de riesgo, es susceptible a acciones de mejora*
Alto – A	*Riesgos que deben tratados a corto plazo*
Extremo - E	*Nivel de riesgo que debe ser tratados con urgencia*

Tabla 7: Definición aceptabilidad el riesgo

El mapa de riesgos quedaría de la siguiente forma:

ACEPTABILIDAD DEL RIESGO						
Probabilidad	valor	Consecuencia				
		1	2	3	4	5
Casi seguro	5	A	A	E	E	E
Probable	4	M	A	A	E	E
Posible	3	B	M	A	E	E
Improbable	2	B	B	M	A	E
Raro	1	B	B	M	A	A

Figura 15: Mapa de aceptabilidad del riesgo

e) Tratamiento del riesgo

*Para el tratamiento, se tendrán en cuenta **solo** los riesgos catalogados como Altos o Extremos, esto es, los riesgos que tienen un nivel superior al aceptable, dado que los demás estaría aceptados acorde a la definición del numeral anterior, para el tratamiento tendremos los siguientes mecanismos:*

- *Reducir la probabilidad:*
  - *Se deben buscar mecanismos que ayuden a reducir la probabilidad de ocurrencia, puede ser a través de auditorías preventivas, formación y sensibilización, mantenimientos preventivos, contratos, pruebas de seguridad (intrusión), etc.*
  - *Así mismo, esta la implementación de controles detectivos, correctivos y disuasivos.*
- *Reducir el impacto*
  - *Para la reducción del impacto es posible desarrollar planes de contingencia y continuidad del negocio, control de fraudes, controles técnicos y administrativos, etc.*
  - *Así mismo, esta la implementación de controles detectivos, correctivos y disuasivos.*
- *Transferir total o parcialmente*
  - *Para la transferencia del riesgo podemos recurrir a pólizas y seguros, acuerdos de confidencialidad, transferencia física a otros lugares (división del riesgo), etc.*
- *Evitar*
  - *Es la decisión tomada de no iniciar o continuar con la actividad que lo origino.*
- *Asumir: Para este tipo de tratamiento estaríamos considerando el **riesgo residual**, que, luego de realizar las diferentes acciones debemos retenerlo o aceptarlo. Aplicaría en primera instancia los riesgos bajos y moderados.*

Luego de seleccionar las medidas de tratamiento, es necesario preparar e implementar los planes para el tratamiento de dichos riesgos:

RIESGOS ALTOS (Naranjas y rojos)	TRATAMIENTO			
	Aceptarlo	Evitarlo	Controlarlo	Transferirlo
Amenaza 3 -- Activo 2			x	
Amenaza 6 -- Activo 3			x	
Amenaza 2 -- Activo 2			x	
Amenaza 3 -- Activo 1			x	
Amenaza 3 -- Activo 4				x

Figura 16: Ejemplo tratamiento de riesgo

Así mismo, es necesaria la creación de proyectos de implementación asociados a los planes de tratamiento, donde estén considerados los diferentes controles a implementar. Dichos planes deberían estar integrados con los planes de gestión de la organización (así no quedarían desarticulados).

f) Monitoreo y revisión

Las revisiones continuas de los riesgos son esenciales para su gestión, de la misma forma, determinar la periodicidad de dicha revisión, no solo para los altos sino también para los niveles aceptables (validando que éstos se mantengan en el nivel de aceptable) y

detectando a tiempo los riesgos emergentes (aquellos nuevos que surgen por cambios de tecnología, por ejemplo).

En esta etapa se define cada cuando se revisaran los riesgos y la gestión de riesgos como tal, para nuestro caso, el mapa de riesgos se revisará cada año (como mínimo) y los riesgos altos (naranjas y rojos) cada 2 meses se harán seguimientos.

12. Declaración de aplicabilidad

Para el SGSI se han seleccionado todos los controles a ser implementados, en el anexo 9 se puede consultar el detalle de la declaración de aplicabilidad, en su versión 1.0

Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad y documentación relacionada de cómo se implementará.

13. Gestión de riesgos

Teniendo en cuenta la guía para calificar riesgos (Anexo 8), se realizó la respectiva evaluación obteniendo los siguientes resultados:

a) Plan de comunicación

Plan de comunicación		
Medio	**Días**	**Frecuencia**
Reuniones	*3 x semana*	*2 horas*
Correo	*Continuo*	
Actas		*acorde a las reuniones*

Tabla 8: Plan de comunicación para gestión de riesgo

b) Activos de información identificados

Se han identificado el siguiente listado de activos, así mismo, para cada activo se le ha dado un nivel de criticidad con el fin de considerar su importancia y prioridad a la hora de realizar un tratamiento de riesgo:

Tipo	**ACTIVOS /RECURSOS**	**Niveles de criticidad**
Medio ambiente e infraestructura	Instalaciones físicas- Centro procesamiento	Alto - A
	Equipamiento auxiliar: Aire acondicionado, potencia,	Alto - A
Personas	Empleados, contratistas, proveedores	Medio - ME
Hardware	Servidores de Bases de Datos y aplicaciones (hardware)	Alto - A
	Medios magnéticos y de almacenamiento	Alto - A
	Computadores, Portátiles, Smartphone	Medio - ME
Software	Aplicación de Bases de Datos	Medio - ME
	Aplicaciones ERP-CRM-OSS y facturación	Alto - A
	Aplicaciones Web	Muy alto - MA
	Sistemas operativos	Alto - A
Comunicaciones	Router, Switch, CPE	Medio - ME
Documentos/datos/información	Acuerdos de Confidencialidad - contratos	Medio - ME
	Datos	Alto - A

Tabla 9: Listado de activos con nivel de criticidad

Cada grupo de activos contiene los elementos asociados al alcance del SGSI, desde los equipos de comunicaciones, pasando por los utilities hasta llegar a las diferentes aplicaciones.

c) Amenazas identificadas

El siguiente es el listado de amenazas para el alcance dado, además, éstas se puede consultar en el anexo 8 "Guia calificar riesgo", en la hoja "Inventario Amenazas":

AMENAZAS TIC	AMENAZAS NATURALES/tecnológicas	AMENAZAS HUMANAS/SOCIALES	AMENAZAS ESTRATÉGICAS Y ADMINISTRATIVAS	AMENAZAS ASOCIADAS A LOS PROYECTOS
Manipulación de datos o software	Inundación	Vandalismo	Violación de derechos de autor	Brecha en la legislación
Manipulación de equipo informático	rayos	Acceso no autorizado al sitio/edificio/sala	Selección de contratistas o personal no idóneo	Errores de diseño
Falla/degradación de equipo informáticoo de comunicación	incendio	Robo		Fraude en la selección de proveedor
Uso no autorizado de software	Falla en aire acondicionado	Ingenieria social		
Suplantación	Fallo en suministro de energia	Error humano		
Acceso no autorizado a red		Empleado descontento		
Software malicioso				
crakeo de contraseñas				
Ataque de negación de servicio				
Deterioro/degradación				
Eliminación no autorizada				
Hacker/cracker				
Cross Site Scripting - XSS				
SQL Injection				
Copias de seguridad incompletas				
Interceptación de datos				

Tabla 10: Listado de amenazas

d) Escenarios de riesgos

En el anexo 8 "Guia calificar riesgo", en la hoja "Agentes" es posible consultar la siguiente información:

- *Escenario de riesgos: Un escenario de riesgos es conjugación de una amenaza sobre un activo, la cual podría eventualmente explotar una o varias vulnerabilidades, para ello, se hace un cruce de la afectación de amenazas vs. Activos, acorde al posible impacto directo que se pueda dar.*
- *Agente generador: Ente externo al sistema con potencial daño.*
- *Causa o vulnerabilidad: Hueco o fallo de seguridad. Motivo, razón o circunstancia por lo que puede consolidarse el riesgo.*
- *Impactos: Posibles efectos o consecuencias que puede generar las amenazas.*
- *Controles actuales: Son los diferentes controles que están implementados y que pueden ejercer cambios sobre la calificación de los escenarios de riesgos.*

Los escenarios se verán de la siguiente forma:

Escenario del riesgos	Agente Generador	Causa	Posibles Impactos generados	Controles actuales
Manipulación de datos o software -- Medios magnéticosy de almacenamiento	Empleados y contratistas con acceso	Falta de control de acceso fisico/lógico, falta de procedimientos de operación	Pérdidas económicas, pérdida de información, pérdida de integridad de datos..	Control de permisos de administración local, personal autorizado para manipulación de cintas y medios, capacitación.
Manipulación de datos o software -- Aplicación de Bases de Datos	Empleados y contratistas con acceso, programas (scripts), códigos maliciosos	Falencia en el control lógico, falta de procedimientos de control de acceso, falencias en el control de ejecución de script, falta de monitoreo del sistema.	Pérdidas económicas, pérdida de información, pérdida de integridad de datos, fraudes.	Definición de roles de acceso, control de acceso lógico, personal idóneo y capacitado.
Manipulación de datos o software -- Aplicaciones ERP-CRM-OSS y facturación	Empleados y contratistas con acceso, programas (scripts), códigos maliciosos	Falencia en el control lógico, falta de procedimientos de control de acceso, falencias en el control de ejecución de script, falta de monitoreo del sistema. No definición adecuada de roles de acceso. Falta de gestión de la vulnerabilidad técnicas.	Pérdidas económicas, pérdida de información, pérdida de integridad de datos, fraudes.	Definición de roles de acceso, control de acceso lógico, personal idóneo y capacitado.
Manipulación de datos o software -- Aplicaciones Web	Empleados y contratistas con acceso, programas (scripts), códigos maliciosos, hackers/crackers	Falencia en el control lógico, falta de procedimientos de control de acceso, falencias en el control de ejecución de script, falta de monitoreo del sistema.No definición adecuada de roles de acceso.Falencias en el acceso remoto.	Daño a la imagen y pérdida de credibilidad, Pérdidas económicas, pérdida de información, pérdida de integridad de datos..	Definición de roles de acceso, control de acceso lógico, personal idóneo y capacitado.
Manipulación de datos o software -- Router, Switch, CPE	Clientes y empleados.	Falta de seguridad dentro de la configuración del Router. Carencia de controles en las cuentas de los funcionarios que manipulan el sistema. Falta de control sobre los puertos y mantenimiento de la configuración, falencias en la aceptación de los sistemas.	Pérdida de paquetes y de disponibilidad, Pérdidas económicas, pérdida de información, pérdida de integridad de datos..	Implementación de lineamientos de seguridad técnica.

Tabla 11: Escenarios de riesgo

e) Mapa de riesgos

Acorde a la fase "Evaluación del riesgo" de la ISO 31000, el siguiente gráfico representa la distribución porcentual del riesgo ya evaluado:

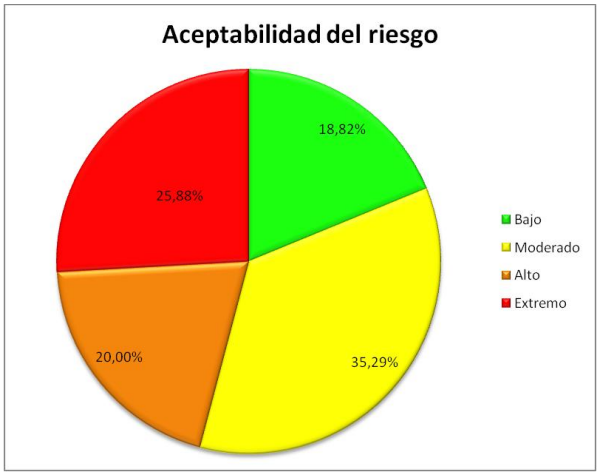

Figura 17: Aceptabilidad del riesgo

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	18.82	16
Moderado	35.29	30
Alto	20.00	17
Extremo	25.88	22

Figura 18: Distribución porcentual del riesgo

*Para lo cual, el 25,88% de los riesgos identificados son **extremos**, implica esto que es necesario establecer mecanismos rápidos de validación/verificación de los controles actuales y proponer controles que nos permitan reducir el nivel de exposición.*

*Por otro lado, el 20.0% de los riesgos totales son **altos,** para éstos se debe establecer mecanismos de corto plazo que permita, de igual manera, la reducción de los riesgos.*

*Dentro de los riesgos **extremos** identificados, se tiene:*

Riesgo	Nivel	Nivel de criticidad del activo
Manipulación de datos o software -- Aplicaciones ERP-CRM-OSS y facturación	*Extremo*	*Alto - A*
Manipulación de equipo informático -- Computadores, Portátiles, Smartphone	*Extremo*	*Medio - ME*
Manipulación de equipo informático -- Router, Switch, CPE	*Extremo*	*Medio - ME*
crakeo de contraseñas -- Computadores, Portátiles, Smartphone	*Extremo*	*Medio - ME*
crakeo de contraseñas -- Aplicaciones Web	*Extremo*	*Muy alto - MA*
Ataque de negación de servicio -- Aplicaciones Web	*Extremo*	*Muy alto - MA*
Cross Site Scripting - XSS -- Aplicaciones Web	*Extremo*	*Muy alto - MA*
SQL Injection -- Aplicación de Bases de Datos	*Extremo*	*Medio - ME*
SQL Injection -- Aplicaciones Web	*Extremo*	*Muy alto - MA*
rayos -- Servidores de Bases de Datos y aplicaciones (hardware)	*Extremo*	*Alto - A*
Acceso no autorizado al sitio/edificio/sala -- Instalaciones físicas- Centro procesamiento	*Extremo*	*Alto - A*
Robo -- Computadores, Portátiles, Smartphone	*Extremo*	*Medio - ME*
Robo -- Router, Switch, CPE	*Extremo*	*Medio - ME*
Robo -- Datos	*Extremo*	*Alto - A*
Error humano -- Empleados, contratistas, proveedores	*Extremo*	*Medio - ME*
Violación de derechos de autor -- Datos	*Extremo*	*Alto - A*
Selección de contratistas o personal no idóneo -- Acuerdos de Confidencialidad - contratos	*Extremo*	*Medio - ME*
Brecha en la legislación -- Acuerdos de Confidencialidad - contratos	*Extremo*	*Medio - ME*
Manipulación de equipo informático -- Sistemas Operativos	*Extremo*	*Alto - A*
Uso no autorizado de software -- Sistemas Operativos	*Extremo*	*Alto - A*
Copias de seguridad incompletas -- Sistemas Operativos	*Extremo*	*Alto - A*
Violación de derechos de autor -- Sistemas Operativos	*Extremo*	*Alto - A*

Tabla 12: Riesgos catalogados extremos

De la misma manera, los riesgos catalogados como "altos" son:

Riesgo	Nivel	Nivel de criticidad del activo
Manipulación de datos o software -- Router, Switch, CPE	*Alto*	*Medio - ME*
Manipulación de equipo informático -- Datos	*Alto*	*Alto - A*
Uso no autorizado de software -- Aplicación de Bases de Datos	*Alto*	*Medio - ME*

Suplantación -- Empleados, contratistas, proveedores	*Alto*	*Medio - ME*
Suplantación -- Aplicaciones Web	*Alto*	*Muy alto - MA*
Ataque de negación de servicio -- Aplicación de Bases de Datos	*Alto*	*Medio - ME*
Eliminación no autorizada -- Datos	*Alto*	*Alto - A*
Hacker/cracker -- Aplicaciones Web	*Alto*	*Muy alto - MA*
Copias de seguridad incompletas -- Medios magnéticosy de almacenamiento	*Alto*	*Alto - A*
Copias de seguridad incompletas -- Datos	*Alto*	*Alto - A*
Inundación -- Instalaciones físicas- Centro procesamiento	*Alto*	*Alto - A*
Ingenieria social -- Empleados, contratistas, proveedores	*Alto*	*Medio - ME*
Error humano -- Datos	*Alto*	*Alto - A*
Empleado descontento -- Computadores, Portátiles, Smartphone	*Alto*	*Medio - ME*
Empleado descontento -- Datos	*Alto*	*Alto - A*
Selección de contratistas o personal no idóneo -- Empleados, contratistas, proveedores	*Alto*	*Medio - ME*
Fraude en la selección de proveedor -- Empleados, contratistas, proveedores	*Alto*	*Medio - ME*

Tabla 13: Riesgos catalogados en alto

f) Mecanismo de tratamiento del riesgo

En el anexo 8 "Guia calificar riesgo", en la hoja "tratamiento" es posible consultar las medidas respectivas sobre los mecanismos de tratamientos propuestos para los riesgos que están por encima del nivel de aceptabilidad.

En general, para todos los riesgos se proponen mecanismos para reducir la probabilidad y/o el impacto, esto se hace buscando controles sobre el agente generador, la causa (o vulnerabilidad) y/o el efecto.

Las diferentes medidas de tratamiento estarán basadas en la norma ISO/IEC 27001 e ISO/IEC 27002 y serán abordados en los proyectos.

14. Propuesta de proyectos a trabajar

Teniendo en cuenta los niveles de riesgos y los diferentes tratamientos que deben realizarse, los siguientes son los proyectos planteados que buscan reducir los diferentes riesgos encontrados. En el anexo 10 se puede encontrar el detalle de los proyectos, así como el cronograma propuesto para su revisión/implementación.

Resumen de proyectos	
Proyecto 1: Corto-mediano plazo	Gestión de la organización de seguridad, políticas y cumplimiento
Proyecto 2: Mediano plazo	Segurida física, ambiental y de los recursos humanos.
Proyecto 3: Mediano-largo plazo	Controles asociados a las Comunicaciones y operaciones
Proyecto 4: Corto-mediano plazo	Clasificación y gestión de activos y Control de acceso
Proyecto 5: Corto mediano - plazo	Control sobre aplicaciones y desarrollo de software en general
Proyecto 6: Largo plazo	Continuidad del negocio e incidentes de seguridad

Tabla 14: Resúmenes de proyectos

15. Auditoría de cumplimiento

La auditoria de cumplimiento se hace sobre los 11 dominios de la norma ISO/IEC 27001:2005, evaluado bajo el modelo de madurez de capacidad CMM a los 133 controles de la norma ISO/IEC 27002:2005.

Para ello, en el anexo 12 "Anexo 12- Informes finales de auditoria-diligenciado.docx" podemos visualizar el informe de dicha auditoria.

El modelo de madures – CMM es un modelo de evaluación de procesos de una organización[12], desarrollado en 1986 el cual establece una serie de prácticas y niveles en los procesos (5 en total), de modo que se tenga un nivel de medición acorde a la evolución de estos, los niveles estipulados son:

- *Inicial*
- *Repetible*
- *Definido*
- *Gestionado*
- *Optimizado*

Con estos niveles, el modelo CMM da cuenta del progreso en los procesos y como las organizaciones van evolucionando en su que hacer. A medida que los niveles aumentan o son alcanzados por las organizaciones, aumenta en igual medida en nivel de

[12] Tomado y ajustado de http://www.globales.es/imagen/internet/Informaci%C3%B3n%20General%20CMMI.pdf

documentación y soporte que debe gestionarse. La siguiente gráfica ilustra el proceso de madurez[13]:

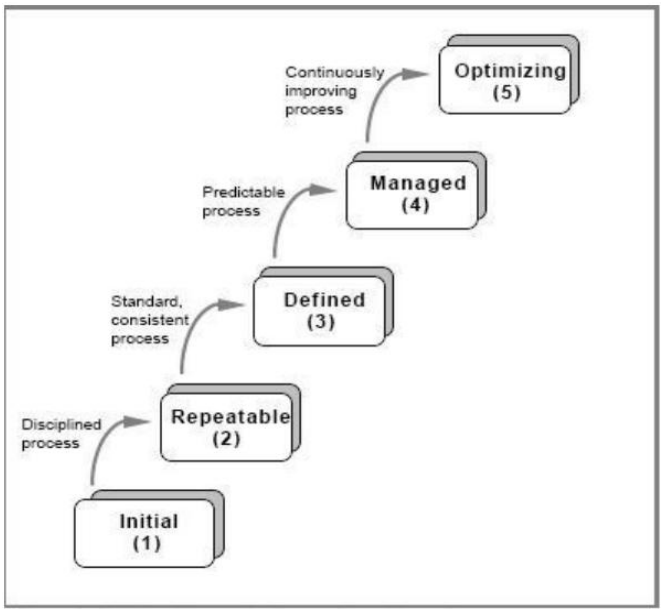

Figura 19: Descripción modelo de madurez - CMM

Para la evaluación de los controles de la norma ISO/IEC 27001:2005, se tomó cada uno de los controles y se calificaron acorde a la siguiente tabla:

Efectividad	CMM	Significado	Descripción
0%	**L0**	*Inexistente*	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	*Inicial / Ad-hoc*	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.

[13] Tomado de http://carlosfau.com.ar/nqi/nqifiles/CMM-Informe.pdf

95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 15: Niveles de calificación madurez CMM

En el anexo 12 podemos entonces revisar los resultados.

16. Conclusiones

Hemos podido observar como desde una manera general se da una descripción de una empresa típica de telecomunicaciones y la necesidad de proteger la información en éste tipo de sector, el cual tiene la obligación de dar cumplimiento a leyes del estado, así como a elementos contractuales y promesas de servicios hacia los clientes.

Para el cumplimiento de estas obligaciones se hace necesario establecer un modelo de seguridad que permita guiar las directrices dadas, por ello, la mejor opción es la norma ISO/IEC 27001, la cual, contempla 11 dominios, 39 objetivos de controle y 133 controles agrupados en su anexo A (ISO/IEC 27002).

Es importante obtener como elemento primario, una evaluación base sobre el estado de la seguridad en la empresa antes de emprender la implementación de la norma, dicha seguridad se ve mejorada en una segunda evaluación desarrollado sobre activos ya identificados, para lo cual, a través de un análisis de riesgo se pudo identificar de manera más clara los posibles impactos negativos que pueden tener y gracias a una ejecución de controles de manera temprana se pudo aumentar los niveles de seguridad.

Así mismo, se ha entregado un plan de tratamiento de riesgo sobre los activos de información, con una propuesta clara proyectada en el tiempo, con recursos y posible presupuesto. Dichos proyectos son fundamentales en su ejecución, toda vez que de esto depende el éxito de la implementación de la norma y el cumplimiento a las partes interesadas que la empresa debe cumplir.

Por último, es importante indicar que, sin el apoyo de la alta dirección, las diferentes áreas impactadas y una metodología para el análisis y tratamiento de riesgos, los proyectos que se enfocan a mejorar los niveles de seguridad tendrían dificultades para su implementación y con ello. Es fundamental para la mitigación de riesgos en seguridad de la información contar un modelo a seguir, y la más indicada en la norma ISO/IEC 27001.

Anexos

El siguiente es el listado de anexos que están asociados en todo el documento.

Anexo 1: Grafico del análisis referencial

Los resultados se obtuvieron calificando cada uno de los controles vs. Los diferentes elementos de seguridad implementados en la empresa, con los siguientes resultados:

ISO 27001			
Numeral	Dominio	Porcentaje cumplimiento	Nivel Ideal
4.2	Establecer y manejar el SGSI	13,0%	100%
4.3	Requerimientos de documentación	8,3%	100%
5	Responsabilidad de la gerencia	25,0%	100%
6	Auditorias Internas SGSI	25,0%	100%
7	Revisión gerencial SGSI	11,7%	100%
8	mejoramiento del SGSI	5,0%	100%

Tabla 16: Resumen calificación ISO 27001

Para el anexo A de la norma se obtuvo:

ISO 27002		
Numeral	**Dominio**	**Porcentaje cumplimiento**
A.5	A.5 Politicas de seguridad	100,00%
A.6	A.6 Organización de la seguridad de la Información	40,91%
A.7	A.7 Gestión de activos	41,00%
A.8	A.8 Seguridad de los recursos humanos	55,56%
A.9	A.9 Seguridad física y ambiental	83,46%
A.10	A.10 Gestión de las comunic y oper	57,50%
A.11	A.11 Control de acceso	62,20%
A.12	A.12 Adquisición, dllo y mante. de SI	57,81%
A.13	A.13 Gestión de incidentes de seguridad de la información	57,00%
A.14	A.14 Gestión de la continuidad del negocio	60,00%
A.15	A.15 Cumplimiento	59,50%

Tabla 17: Resumen calificación ISO 27002

Se anexa a éste proyecto el archivo Excel "Anexo 1 -Analisis-referencial-controles-iso27001" con la calificación inicial.

Anexo 2: Políticas de seguridad

En el documento anexo se pueden encontrar las políticas de seguridad de la información para al SGSI.

Anexo 3: Formato Informe final de la auditoria

En el fichero Word anexo se encuentra la estructura de informe final de auditoría.

Anexo 4: Cronograma propuesto para la Auditoria

	Nombre de la tarea	Duración	Inicio	Finalizar	Predecesoras
1	**Plan de auditoria SGSI-UOC**	60	01/07/14	22/09/14	
2	Conformación del equipo de trabajo	6	01/07/14	08/07/14	
3	Inicio de la auditoria	2	09/07/14	10/07/14	
4	Presentación del proyecto	1	09/07/14	09/07/14	2
5	Firma del acta de inicio	1	10/07/14	10/07/14	4
6	Planificación	6	08/07/14	15/07/14	
7	Reunión con el equipo de trabajo (auditores y auditados) y definición alca	6	08/07/14	15/07/14	
8	Creación/ajuste del cronograma	3	08/07/14	10/07/14	
9	Documentación de las pruebas	3	10/07/14	14/07/14	
10	Entrega del cronograma ajustado para su aprobación	1	15/07/14	15/07/14	9
11	Pruebas	41	15/07/14	09/09/14	
12	Recolección de información	3	15/07/14	17/07/14	
13	Entorno interno y regulación, identificación público Objetivo	3	15/07/14	17/07/14	
14	Estudio de información recolectada	1	16/07/14	16/07/14	
15	Ejecución de la pruebas	33	18/07/14	02/09/14	
16	Revisión de actas, acuerdos y conformación del SGSI	2	18/07/14	21/07/14	
17	Revisión de informes de riesgos y políticas	3	21/07/14	23/07/14	
18	Revisión de controles ISO/IEC 27001 implementados	5	21/07/14	25/07/14	
19	Revisión de condiciones técnicas y casos de uso	2	26/07/14	28/07/14	
20	Ejecución técnica de pruebas: Análisis de vulnerabilidades y ethical hac	30	18/07/14	28/08/14	
21	Entrega de informes preliminares	3	29/08/14	02/09/14	20
22	Análisis de la documentación	13	23/08/14	09/09/14	
23	Revisión de documentación	2	03/09/14	04/09/14	21
24	Ejecución de entrevistas y visitas	8	23/08/14	02/09/14	
25	Pruebas técnicas: Análisis de vulnerabilidades	4	03/09/14	08/09/14	21
26	Reunión de seguimiento de auditoria	1	09/09/14	09/09/14	25
27	Elaboración de informes	5	10/09/14	16/09/14	26
28	Presentación de informes	1	17/09/14	17/09/14	27
29	Cierre de auditoria	3	18/09/14	22/09/14	
30	Generación de informe de cierre	2	18/09/14	19/09/14	28
31	Generación de cronograma de revisión anual/semestral del SGSI	1	22/09/14	22/09/14	30

Figura 20: Cronograma propuesto para la auditoria

Anexo 5: Tabla de indicadores

En el archivo Excel anexo, se puede revisar todos los indicadores para el SGSI.

Anexo 6: Presentación revisión por la dirección

En la presentación PowerPoint se puede ilustrar la plantilla para la presentación a la alta gerencia.

Anexo 7: Formato actas de reunión

Éste formato nos sirva para la documentación de las diferentes actas, en especial, las de los comité de gerencia y de seguridad.

Anexo 8: Guía para calificar riesgos

Éste archivo Excel nos permitirá de manera más práctica para realizar la calificación de los riesgos.

Anexo 9: Declaración de aplicabilidad

En el fichero Excel anexo se encuentra la declaración de aplicabilidad en su versión 1.0, la cual puede verse así:

Declaración de aplicabilidad				
Versión 1,0				
Numeral	**Dominio o descripción**	**Aplica**		**Evidencia o registro de implementación**
A.5	Politicas de seguridad	Aplica		
A.5.1.1	Documento de la política de seguridad de la información.	Si	Tiene una aplicabilidad global en todo el SGSI	Documento de política firmado por la alta dirección
A.5.1.2	Revisión de la política de seguridad de la información.	Si	De manera periódica se debe realizar la revisión y documentar las acciones de mejora	Actas de revisión periódica
A.6	Organización de la seguridad de la Información			
A.6.1.1	Compromiso de la dirección con la seguridad de la información	Si	Es fundamental, dado que tienen la responsabilidad de aprobar el SGSI como última instancia.	Actas de comité
A.6.1.2	Coordinación de la seguridad de la información.	Si	Debe haber un área que lidere la implementación del SGSI	Equipo de trabajo conformado

Figura 21: Muestra de la declaración de aplicabilidad.

Anexo 10: Proyectos del SGSI

En el fichero Excel anexo 10 se encuentra la descripción de los diferentes proyectos que buscan la validación/implementación de controles de la norma ISO/IEC 27001, con el objetivo de reducir los riesgos encontrados.

Por otro lado, el siguiente es el cronograma propuesto: Diagrama de Gantt

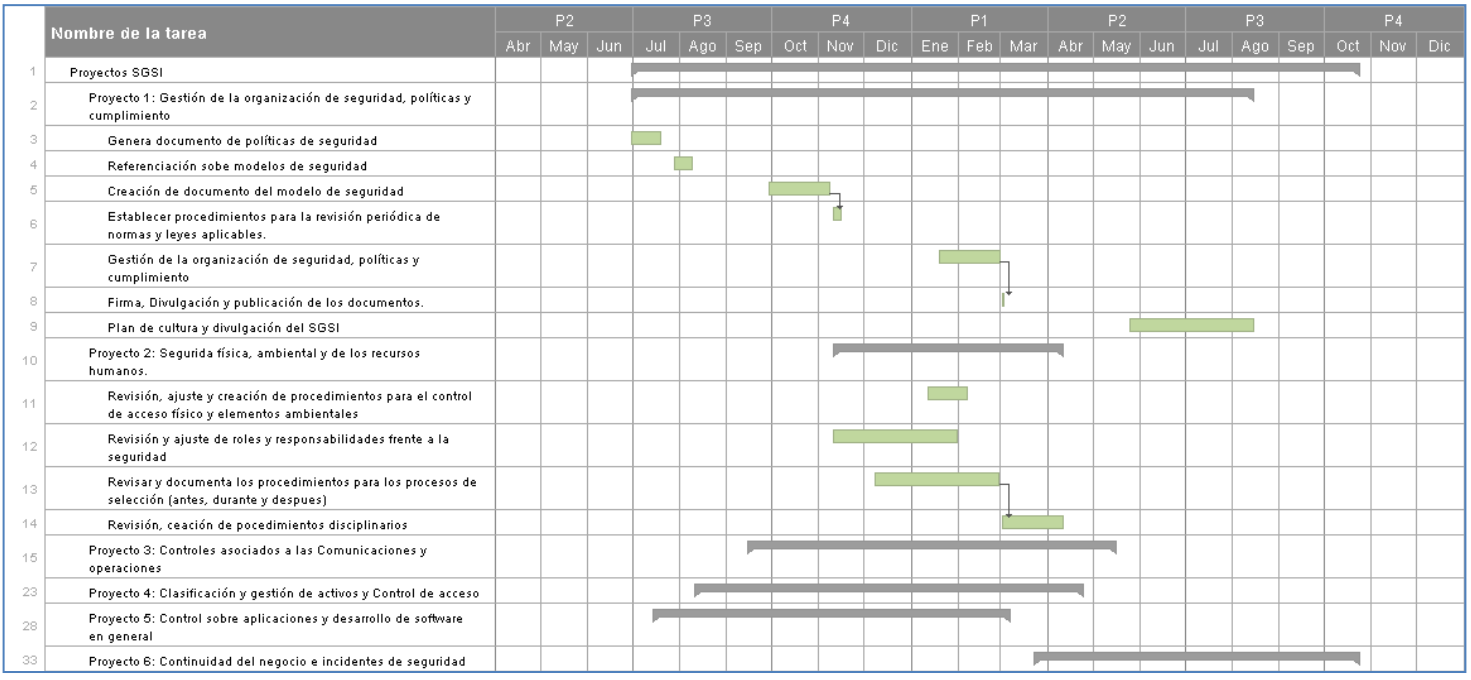

Figura 22: Diagrama de Gantt para los proyectos.

Anexo 11: Medición de madurez CMM

En éste anexo, que es un archivo Excel podemos encontrar la calificación de los controles de la norma ISO/IEC 27002:2005 bajo el modelo de madurez CMM.

Anexo 12: Informe final de la auditoria

En éste anexo "Informes finales de auditoria-diligenciado.docx" podemos encontrar el informe final diligenciado (haciendo uso del anexo 3), como resultado de la medición (anexo 11).

Glosario

Declaración de aplicabilidad: *Es un documento donde se expresa cuales controles de la norma se van a implementar y los no seleccionados, se debe indicar porque no.*

Riesgo[14]*: Evento no rutinario que en el momento que suceda, puede generar impactos negativos en los proceso y/o los objetivos del negocio. Efecto de la incertidumbre sobre los objetivos.*

Gestión del Riesgo: *Acorde a la norma ISO/IEC 31000, la gestión de riesgo es*[15] *"Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo".*

Confidencialidad[16]*: La propiedad que esa información esté divulgada y no sea divulgada a personas, entidades o procesos no autorizados.*

Integridad[17]*: La propiedad de salvaguardar la exactitud e integridad de los activos.*

Disponibilidad[18]*: La propiedad de estar disponible y utilizable cuando se requiera una entidad autorizada.*

CRC: *Comisión de regulación de comunicaciones de Colombia.*

Política de seguridad: *Documento aprobado por la alta gerencia que expresa de manera ética y responsable, lo que se puede o no realizar con respecto a la seguridad de la información.*

Indicador: *Mecanismo de medición o comparación de resultado, con el fin de obtener el nivel de efectividad de cumplimiento de acciones implementadas, ésta se obtiene a partir de calificaciones.*

Efecto o consecuencia: *Impacto negativo que tiene un sistema.*

Probabilidad: *Posibilidad de que ocurra un evento, la cual esta medida en porcentaje.*

Riesgo residual: *Riesgo resultante después de ejecutar medidas de tratamiento.*

Riesgo aceptable o nivel aceptable del riesgo: *Es aquel riesgo que, una vez calificado, su nivel de impacto puede ser tolerado por la organización, esto es, se acepta y se asume.*

---

[14] Creado con datos propios y de Norma Técnica Colombiana NTC-ISO 31000. (2011). Recuperado de http://tienda.icontec.org/brief/NTC-ISO31000.pdf

[15] Norma Técnica Colombiana NTC-ISO 31000. (2011). Recuperado de http://tienda.icontec.org/brief/NTC-ISO31000.pdf

[16] Tomado literal de ISO/IEC 27001, Recuperado de http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html

[17] Ídem.

[18] Ídem.

Aceptación del riesgo*: Acción o decisión de aceptar las consecuencias o posibilidades que un riesgo se materialice.*

Gestión del riesgo[19]*: "La administración del riesgo es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones."*

Agente generador*: Ente externo al sistema con potencial daño.*

Causa o vulnerabilidad*: Hueco o fallo de seguridad. Motivo, razón o circunstancia por lo que puede consolidarse el riesgo.*

Escenario de riesgo*: Es el riesgo en sí, es la combinación de un conjunto de amenazas que pueden causar un impacto negativo en los activos, acorde a al vulnerabilidades explotadas.*

[19] Tomado textual de Norma ***AS/NZS 4360.*** ***http://www.bcu.gub.uy/Acerca-de-BCU/Concursos/Est%C3%A1ndar%20Australiano_Adm_Riesgos.pdf***

Bibliografía

1. *CAO Avellaneda, Javier (03-09-2007). "Estándar ISO/IEC 2001, Primera edición 2005-10-15 en castellano" [Artículo en línea]. Recuperado de http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html y de http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf.*
2. *TMFORUM (2014).The Business Process Framework (eTOM). Recuperado de http://www.tmforum.org/businessprocessframework/1647/home.html*
3. *Campo Muñoz, Wilmar Yesid (19-dic-2012). Introducción al eTOM. Recuperado de http://dtm.unicauca.edu.co/pregrado/conmutacion/transp/10-eTOM.pdf*
4. *Unión Internacional de Telecomunicaciones – ITU-T. (2008).M.3050-Mapa de operaciones de telecomunicación mejorado. Recuperado de http://www.itu.int/rec/T-REC-M.3050/es*
5. *Cano Martínez, Jeimy. Sauce Mesa, Gabriela y Prandini, Patricia. (2013) ACIS- V encuesta latinoamericana de seguridad de la información. Recuperado de http://www.acis.org.co/index.php?id=332*
6. *Comisión de Regulación de Comunicaciones de la Republica de Colombia. (2014). República de Colombia, circular 3066 de 2011. Recuperada de http://www.crcom.gov.co/index.php?idcategoria=61450*
7. *Comunidad internacional de implantadores de ISO27000. (2007). Consejos de implantación y métricas de ISO/IEC 27001 y 27002. Recuperado de http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf*
8. *Instituto Colombiano de Normas Técnicas - ICONTEC.(2011). Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo, principios y directrices. Recuperado de http://tienda.icontec.org/brief/NTC-ISO31000.pdf*
9. *Phillips, Ann. Cómo gestionar con éxito una auditoría interna conforme a ISO 9001:2008. AENOR (Asociación Española de Normalización y Certificación), 2010. ISBN: 978-0-87389-751-8. [En línea] Documento recuperado el 2 de Mayo de 2013 en http://www.aenor.es/aenor/inicio/home/home.asp*
10. *Diseño de cronogramas en línea: https://www.smartsheet.com*
11. *Open Web Application Security Project (OWASP). (2014). Proyecto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. Recuperado de https://www.owasp.org/index.php/Main_Page*
12. *Chapin A, David. (2005). ¿Cómo puede medirse la seguridad?. INFORMATION SYSTEMS CONTROL JOURNAL, VOLUMEN 2. Traducido al español por Javier Ruiz Spohr . Recuperado de http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf*
13. *Instituto Argentino de normalización y Certificación- IRAM. (2010). Documento de estudio: Esquema 1 de NORMA IRAM-ISO/IEC 27004. Recuperado de http://www.frlp.utn.edu.ar/materias/habprof/teoria/27004%20IRAM-ISO-IEC.pdf*

14. *Ledesma, Cristina. (2008). Métricas de seguridad. Information security Conference – ISACA. Recuperado de http://www.unit.org.uy/misc/novedades/2008-06-12_Metricas_Unit.pdf*
15. *National Institute of Standards and Technology – NIST (2007). Security Measurement NIST SP 800-55 Revision 1. Recuperado de http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2007-09/Barker_ISPAB_Sept2007-SP800-55R1.pdf*
16. *The Center for Internet Security (2010). The CIS Security Metrics v1.1.0. Recuperado de https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf*
17. *Kosutic, Dejan. (2013). A first look at the new ISO 27001. Recuperado de http://blog.iso27001standard.com/2013/01/28/a-first-look-at-the-new-iso-27001-2013-draft-version/*
18. *Gonzalez Trejo, Dulce. (2013). ISO-27001:2013 ¿Qué hay de nuevo?. Recuperado de http://www.magazcitum.com.mx/?p=2397*
19. *Ministerio de hacienda y administración Pública del Gobierno de España. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Recuperado de https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_II_catalogo.pdf*
20. *Instituto de normas técnicas y certificación – ICONTEC. (2006). RESUMEN NORMA TECNICA COLOMBIANA NTC 52541 (Primera Actualización 2006-09-12) GESTION DE RIESGO. Recuperado de http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf*
21. *Guerrero, David. (2013). Blog NTC-ISO 31000 Mejorado. Recuperado de http://www.slideshare.net/DAFEGUER/ntc-iso31000*
22. *Coggan, John (2012). Catálogo de vulnerabilidades, amenazas y controles para la ISO 27001. Administración de seguridad de información. BSI Brasil Training. Manual de referencia.*
23. *Standars New Zealand (2009). AS/NZS 4360 Estándar Australiano Administración de Riesgos. Recuperado de http://www.bcu.gub.uy/Acerca-de-BCU/Concursos/Est%C3%A1ndar%20Australiano_Adm_Riesgos.pdf y de http://www.standards.co.nz/news/standards-information/risk-managment/*
24. *Smartsheet (2014). Gestor de proyecto en la nube. Recuperado de http://es.smartsheet.com/*
25. *Globales (2007). Capability Maturity Model Integration. CMMi – Anexo 1. Recuperado de http://www.globales.es/imagen/internet/Informaci%C3%B3n%20General%20CMMI.pdf*
26. *Alvaríz; Bilbao; Goñi; Saavedra (2006). CMM – Capability Maturity Model. Ingeniería de Software 2006 – U.N.C.P.B.A. Recuperado de http://carlosfau.com.ar/ngi/ngifiles/CMM-Informe.pdf*