ELABORACIÓN DE UN PLAN PARA LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013

AUTOR: ING. SANDRA MURILLO GUACAS
DIRECTOR: MÁSTER ANTONIO JOSE SEGOVIA HENARES
DICIEMBRE DE 2015

MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

AUTOR: SANDRA MURILLO GUACAS
Ingeniera de Sistemas

DIRECTOR: MÁSTER ANTONIO JOSE SEGOVIA HENARES

Consultor en la asignatura de Sistemas de Gestión de Seguridad de la Información en la UOC.
Miembro del Tribunal Evaluador de los TFM.
Ingeniero Superior en Informática
Ingeniero Técnico en Informática de Sistemas
Máster Seguridad Información - Universidad Politécnica de Madrid
Posgrado Desarrollo de Aplicaciones para Internet y Web Services - Universidad de Sevilla
Posgrado Desarrollo .NET - UOC
Auditor Jefe cualificado por AENOR y AENOR Internacional en ISO 27001.
Participa como Consultor freelance en varios proyectos relacionados con las tecnologías y el mundo de las TIC.

Cali, octubre 16 de 2015

Agradecimientos

Quiero agradecer a todas las personas que de una u otra manera me apoyaron en esta etapa de mi vida, por su comprensión, paciencia y dedicación, en especial a Dios por la oportunidad que me dio y porque nunca me dejó desfallecer, a mis padres porque siempre creyeron en mí y por todo su amor, que me ha ayudado, en mi crecimiento personal y profesional, a mi familia por su voz de aliento, al Ingeniero Edgar Valdés de la Universidad Santiago de Cali, porque siempre estuvo en esos momentos difíciles brindándome su ayuda incondicional, a los profesores, a los tutores y al Director de Trabajo Final de Maestría de la Universidad Oberta de Catalunya por ese excelente nivel académico y las enseñanzas que dejaron en mí.

RESUMEN

La información como uno de los recursos más importante para la gestión en las organizaciones, tiene un valor incalculable, por lo que debe ser debidamente protegida. Según la Norma ISO 27001, la seguridad de la información, consiste en preservar la confidencialidad, integridad disponibilidad, así como también los sistemas que hacen parte de su tratamiento, dentro de la organización.

Garantizar un nivel de protección total de la información es casi imposible, por lo que las empresas deberán estar siempre atentas a cualquier situación que pueda comprometerla, implementando y manteniendo controles para mitigar los riesgos. El camino a seguir es la implementación de un Sistema de Seguridad de La Información que permite que los riesgos a los que se encuentra sometida la información sean conocidos, asumidos y tratados de tal manera que minimicen el impacto que generan a las organizaciones.

En este proyecto se realiza un análisis del estado actual de la Seguridad de la Información en SEIT CONSULTORES CTA, empresa dedicada a la Auditoría y Consultoría Informática. El proceso misional de negocio es el desarrollo de software a la medida y el objetivo del proyecto es el análisis y el diseño de un Plan Director para la implementación del Sistema de Gestión de la Seguridad de la Información en dicha empresa.

ABSTRACT

Information as one of the most important management resources in organizations, is invaluable, so it must be properly protected. According to ISO 27001, the information security is to preserve the confidentiality, integrity, availability, as well as the systems that are part of their treatment within the organization.

Ensure a level of total protection of information is almost impossible, so that companies will always be alert to any situation that might compromise, implement and maintain

controls to mitigate risks. The way forward is to implement a system of information security that enables risks to which the information is subject are known, assumed and treated in such a way that minimizes the impact generated organizations.

In this project an analysis of the current state of information security in SEIT CONSULTANTS CTA, dedicated to the Audit and Consulting is performed. Missionary business process is the development of custom software and the project objective is the analysis and design of a master plan for the implementation of information security management system in the company.

Contenido

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

1. INTRODUCCIÓN

En las empresas de hoy hay conciencia de la importancia de la información como elemento fundamental en el desarrollo de sus actividades y el logro de metas y objetivos, razón por lo cual cada día cobra más importancia su administración. Es en este momento donde la seguridad de la información aparece como una disciplina que pretende mantener la integridad, disponibilidad y la confidencialidad que se requiere en el mundo de hoy.

En este proyecto se presenta el análisis y diseño de un Plan Director de Seguridad de la Información para una empresa de auditoría y consultoría que como nuevo proceso ha incorporado el desarrollo de software.

La dirección de la empresa ha iniciado acciones para lograr como una meta a corto plazo poder garantizar en lo posible operaciones con información segura para sus actividades propias y para las relaciones con sus clientes y terceros.

Para la implementación del SGSI, se ha tomado como base la norma ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, en cuyo plan se definirá la política, los objetivos de seguridad y un análisis Gap de la empresa que permita determinar el nivel seguridad en que se encuentra. También se desarrollará un análisis de riesgos con el que se pueda establecer los controles que alineados a los objetivos corporativos apoyan al desarrollo de las estrategias del negocio.

1.1. Origen e Historia de las normas ISO/IEC 27001 e ISO/IEC 27002

La Norma ISO/IEC 27001, ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora un sistema de gestión de la seguridad de la información (SGSI). Publicada el 15 de

Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de que no es obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001).

La Norma ISO/IEC 27002, publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009. Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002) este estándar ha sido actualizada en 2013 dejando un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013, también traducida al castellano como UNE-ISO/IEC 27002:2015 desde el 1 de julio de 2015.

2. CONTEXTUALIZACIÓN

2.1. ENFOQUE Y DESCRIPCIÓN DE LA EMPRESA

Empresa constituida en el 2009, por un grupo de Ingenieros Profesionales con el propósito de ofrecer Soluciones informáticas en Auditoría, Consultoría y Desarrollo de Software; para organizaciones del sector público y privado. Pertenece al grupo de Cooperativas de Trabajo Asociado, organizaciones sin ánimo de lucro, pertenecientes al sector solidario de la economía, que asocian personas naturales que simultáneamente son gestoras, contribuyen económicamente a la cooperativa y son aportantes directos de su capacidad de trabajo para el desarrollo de actividades económicas, profesionales o intelectuales, con el fin de producir en común bienes, ejecutar obras o prestar servicios para satisfacer las necesidades de sus asociados y de la comunidad en general.

2.1.1. Actividad Específica

Es una empresa dedicada a la Auditoría y Consultoría de Sistemas Informáticos y ante las exigencias del mercado ha visto la oportunidad de incursionar en el desarrollo de software a la medida.

Visión: Ser en los próximos cinco años una organización reconocida a nivel nacional e internacional, ocupando un lugar preferencial en la prestación de Consultoría y Asesoría Informática en empresas nacionales e internacionales.

Misión: Apoyar organizaciones públicas y privadas en la gestión de tecnologías informáticas con soluciones estratégicas, efectivas, herramientas tecnológicas innovadoras y talento humano competente.

2.1.2. Organigrama de la Empresa

A continuación se presenta la estructura de la empresa.

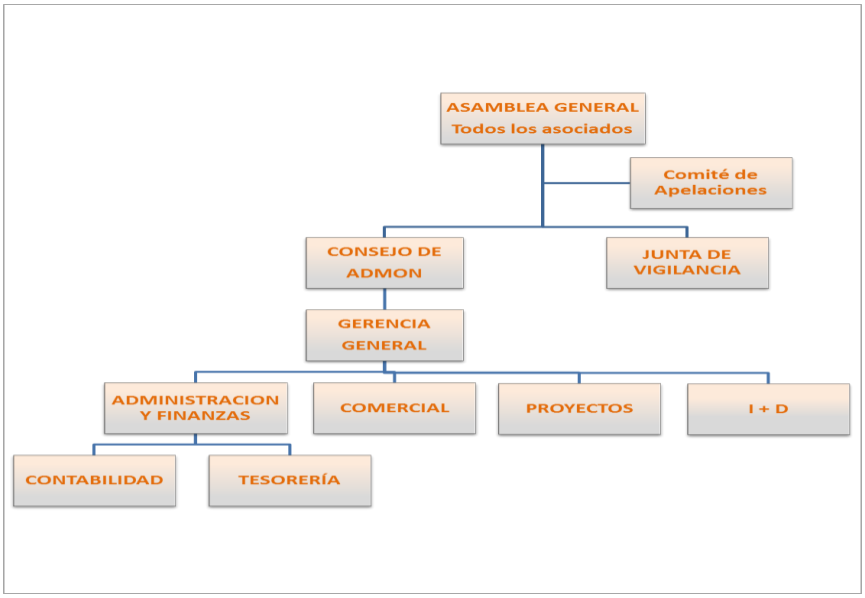

Figura No. 1: Diagrama Organizacional

2.1.3. Funciones de los cargos

- **Asamblea General.** Es el órgano máximo de administración de la Cooperativa y sus decisiones son obligatorias para todos el personal asociados, siempre que se hayan adoptado de conformidad con las normas legales, reglamentarias o estatutarias. La constituye la reunión del personal asociado hábil o de los delegados elegidos por éstos.
- **Comité de Apelaciones.** Para considerar y resolver los recursos de apelación interpuestos por los asociados excluidos, la Asamblea General mediante el procedimiento establecido en el respectivo Reglamento de Asamblea, designará un Comité de Apelaciones, el cual estará integrado por tres (3) asociados hábiles, cuyo período será de un (1) año.

- **Consejo de administración.** Es el órgano permanente de administración de la Cooperativa subordinado a las directrices y políticas de la Asamblea General. Estará integrado por cinco (5) miembros principales y cinco (5) suplentes, elegidos por la Asamblea General, sin perjuicio que puedan ser reelegidos o removidos libremente por ésta.
- **Junta de Vigilancia.** Es el órgano que tiene a su cargo velar por el correcto funcionamiento y eficiente administración de la Cooperativa, referido al control social. Estará integrada por tres (3) asociados hábiles con sus respectivos suplentes, elegidos por la Asamblea General para períodos de dos (2) años, sin perjuicio que puedan ser reelegidos o removidos libremente y responderán ante ella por el cumplimiento de sus deberes, dentro de los límites de la Ley y del Estatuto.
- **Gerencia General.** El Gerente es el Representante Legal de la Cooperativa, principal ejecutor de las decisiones de la Asamblea General y del Consejo de Administración quien lo nombrará.
- **Administración y Finanzas.** Encargada de los procedimientos administrativos que permitan gestionar la administración financiera necesarios para el normal desarrollo de las actividades de la Dirección.
- **Comercial.** Encargada de las actividades de entrega y soporte de los bienes y servicios producidos por la empresa.
- **Proyectos.** Encargada del direccionamiento los proyectos de la empresa
- **I+D.** Se encarga de
- **Contabilidad.** Encargada de la gestión contable.
- **Tesorería.** Encargada de recaudos y pagos

Por el numero de asociados y su capital, en Colombia es considerada como una Microempresa.

Acontinuación se describe La Empersa a través de un esquema las actividades que generan valor (Canena de Valor).

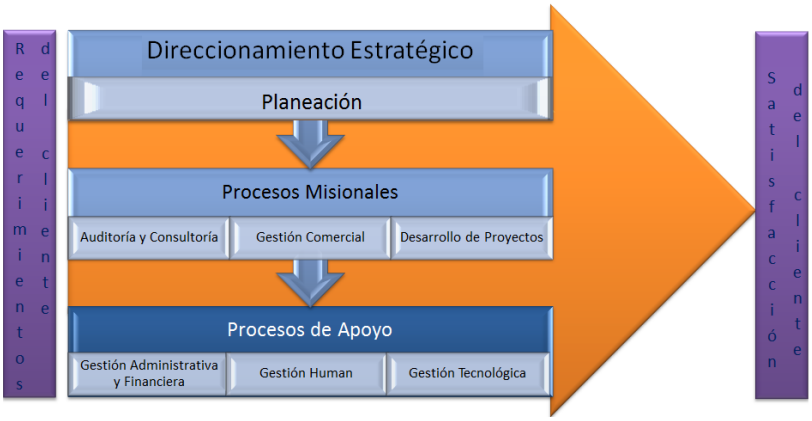

Figura No. 2: La Empresa por Procesos

2.1.4. Políticas de la Empresa

Esta empresa no cuenta con ninguna política, normas y buenas prácticas de seguridad de la información que puedan ofrecer confianza a sus clientes. Las situaciones que se presentan al interior de la organización como conflictos o inconformidades de los clientes son direccionados al Gerente, quien por su vasta experiencia se encarga directamente.

En los últimos años la empresa no ha sido muy rentable, así que se han centrado en atender las ventas más que en otros factores también relevantes como la calidad, la seguridad y un adecuado gobierno corporativo.

Los asociados de la empresa siendo conscientes de la falta de una adecuada gestión de la seguridad, ven la importancia de implantar un Sistema de Gestión de la Seguridad de la información para ser más competitivos.

2.1.5. Arquitectura de la red

El servidor principal se encuentra conectado a internet y solo dispone del firewall por defecto del sistemas operativo, las estaciones se conectan al servidor vía inalámbrica y

todas son locales, no hay conexiones remostas, aunque nunca se han visto amenazados la posibilidad de ataques es alta. Tampoco se dispone de protección frente a alteraciones de fluido eléctrico.

- Cuenta con una oficina en la Ciudad de Cali, departamento del Valle del Cauca.
- En la actualidad tiene 11 asociados y 4 personas externas contratadas para el desarrollo.
- Actualmente sus clientes son empresas del sector público y privado en la república de Colombia con expectativas de expansión al mercado latinoamericano.
- Se cuenta con un sitio Web alojado en un hosting externo, en cuento a software aplicativo se tiene un sistema de información en la nube para la gestión Niif en las microempresas clientes y otros para la gestión contable interna alojada en una estación de trabajo.

Aunque a través del portal Web no se realiza ninguna acción transaccional, si se utiliza para el envío de informes, consultas bancarias, descarga de archivos y mensajes por correos electrónicos.

Del Sistema contable no se obtiene soporte de la casa productora por ser una versión muy antigua, se realizan copias de seguridad que son guardadas en la misma máquina que almacena el Sistema contable. Por ser una entidad sin ánimo de lucro están vigilados por la Super Intendencia de Economía Solidaria, a quien deben reportar la información financiera y contable. Al Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo deben reportar información financiera.

Cuentan con dos Servidores, uno como Servidor de Directorios, de datos, de Impresión y de archivos. El segundo como servidor de desarrollo y de pruebas. El acceso físico al servidor es pleno para cualquier visitante, debido a que no se tiene un sitio separado del área de desarrollo. En cuanto al acceso físico a las oficinas de la empresa, no se garantiza un sistema de seguridad confiable como sistemas de alarmas u otros.

El acceso lógico a los Servidores y estaciones de trabajo está dado por contraseñas que aunque cumple con características adecuadas, nunca se han cambiado, el servidor maneja directorio activo.

En el siguiente diagrama se puede apreciar la infraestructura tecnológica y la configuración de la red.

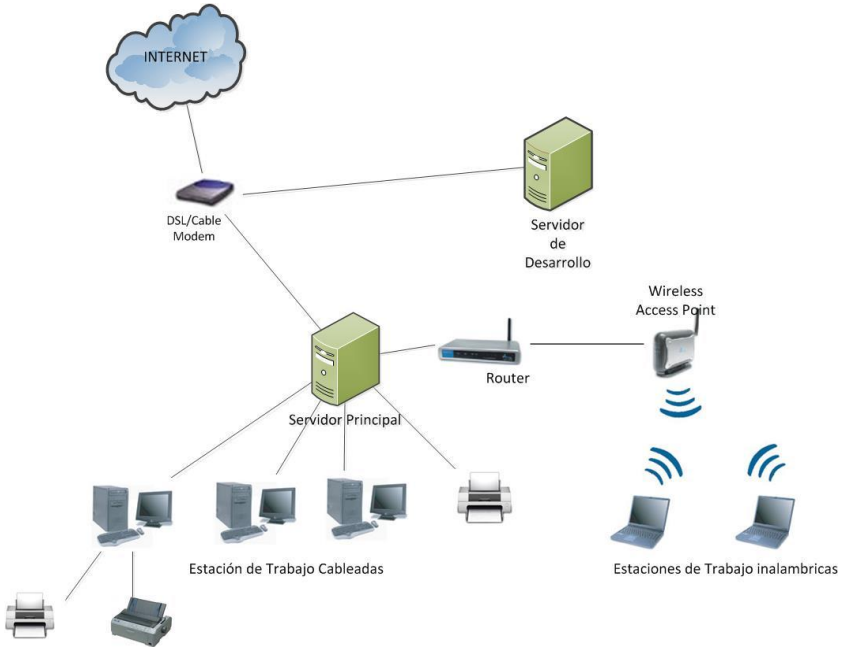

Figura No. 3: Diagrama de Red de la Empresa

A continuación se detalla los recursos con los que cuenta la empresa:

Equipos de Informática		
Equipo	**Cantidad**	**Descripción**
Servidor Principal	1	HP ML-150 G6 - Intel Xeon Quad Core, DD 250 GB, Ram 2 GB Sistema Operativo Windows Server 2008 R2, Procesador 2.0 GHz
Servidor de Desarrollo y Pruebas	1	Clon Sistema Operativo Windows Server 2008 R2, DD 500 GB, Ram 2 GB Procesador 2.41 GHz
Desktop No. 1	1	HP Pro 3000 Small Form Factor PC, Sistema Operativo

		Windows 7 Profesional SP 1, DD 150 GB, Ram 2 GB, Procesador 2.6 GHz
Desktop No. 2	1	Compaq 18 all-in-one, DD 250 GB, Ram 2 GB, Sistema Operativo Windows 8.1 Profesional, Procesador 2.41 GHz
Desktop No. 3	1	DELL H81M-H, DD 1 TB, Ram 4 GB, Sistema Operativo Windows 7 SP 1, Procesador i3 3.6 GHz
Portátil Nos. 4 y 5	2	Compaq Presario CQ40, Proc. AMD Sempron, Ram 2GB, DD 500 GB LCD 14"
Equipos de Red		
Equipo	**Cantidad**	**Descripción**
Cable Modem	1	Modem DSL / ISP
Rourter	1	8 Puertos Cable 10/100Mbps
Access Point	1	dlink dwl-2100ap 108 Mbps
Equipos Auxiliares		
Equipo	**Cantidad**	**Descripción**
Impresora	1	HP Multifuncional photosmart C3180 all-in-one
Impresora	1	HP Multifuncional HP Deskjet 2050
Impresora	1	EPSON LX 300 Matricial
Regulador de Voltaje	3	1000 Watts
Software		
Software	**Cantidad**	**Descripción**
Windows 7 Profesional	2	1 licencia vencida, 1 licencia activa
Windows 8.1	3	Licencias activas
Microsoft Office	5 und	2 licencias activas, 3 vencidas
Antivirus	7 und	4 licencias de uso libres, 3 adquirida
Windows Server 2008 R2	2 und	2 licencias vencidas
J2EE	3 und	Plataforma de programación Java
MyEclipse IDE	1 und	Para desarrollo java, 1 licencia
Eclipse IDE for Java EE Developers	2 und	Para desarrollo java, de uso libre
Aplicativos		
Aplicativos	**Cantidad**	**Descripción**
Aplicación Contable	1	Licencia muy antigua, la empresa desarrolladora ya no brinda soporte.
Aplicación Micronif	1	Aplicativo para generación de Balance Inicial Niif - Desarrollo propio
Sigcoop 8.0	1	Aplicativo para generación de reportes ante la Super Intendencia de Economía Solidaria - Licencia Activa

Tabla No. 1: Tabla de Recursos de Informáticos

2.2. ALCANCE

El desarrollo de software visto como oportunidad de negocio y una actividad de alta competencia, las empresas de este sector buscan posicionamiento en el mercado nacional e internacional. Debido a esto el Plan Director De Seguridad de La Información debe ser un empeño prioritario. En este trabajo se consideran el proceso misional Desarrollo de Proyectos y se formulará el plan para la implementación del SGSI

3. OBJETIVOS DE SEGURIDAD

3.1. OBJETIVO GENERAL

Elaborar un plan para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013.

3.2. OBJETIVOS ESPECIFICOS

- Identificar el contexto de la organización para establecer los riesgos potenciales en el ambiente informático
- Proponer controles para preservar la seguridad de la información durante el ciclo de vida del desarrollo de sistemas de información.
- Establecer controles para preservar la protección de datos durante las pruebas ejecutadas a los sistemas de información.
- Diseñar un plan de concientización sobre la importancia de la Seguridad de la información.
- Establecer los recursos requeridos para la implementación del plan Director

4. ANÁLISIS DIFERENCIAL

Con el fin de determinar el nivel de Seguridad de la Información de acuerdo al estándar ISO/IEC27001:2013 se realiza un GAP Analisys; actividad que permitirá establecer el nivel de madurez de los procesos y determina el esfuerzo necesario para su implementación.

Para ello se revisarán los 14 dominios, 35 objetivos de control y 114 controles especificados en la norma:

A continuación se relacionan los dominios de la Norma**:**

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad delos recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad en las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relaciones con los proveedores
- Gestión de incidentes en la seguridad de la información
- Aspectos de seguridad de la información en la gestión de continuidad de negocio
- Cumplimiento

Para llevar a cabo el diagnostico se entrevistó al Ingeniero responsable del Macroproceso de Gestión Tecnológica y se complementó con evidencias y documentación de los procesos de la cadena de valor.

4.1. CRITERIOS DE EVALUACIÓN

Para valorar el nivel de seguridad actual de la Empresa se realiza la evaluación utilizando el modelo COBIT V4.1 basado en los niveles de madurez, que consiste en una puntuación de 0 a 5, donde el menor cumplimiento es (0): "No existente" y el mayor cumplimiento es (5): "Optimizado".

DESCRIPCIÓN	% DE CUMPLIMIENTO	NIVEL DE MADUREZ
No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver	0%	No existente
Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ***ad hoc*** que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizada	20%	Inicial
Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los error es son muy probables	40%	Repetible
Definido-Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes	60%	Definido
Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmenta	80%	Administrado
Optimizado- Los procesos se han refinado hasta un nivel de mejo r práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida	100%	Optimizado

Tabla No. 2: Niveles de madurez - COBIT V4.1

De acuerdo con esta buena práctica se ha establecido que el promedio de madurez de los procesos a través de las organizaciones del mundo es 3, que representaría metas de 60%.

4.2. GAP ANALISIS

4.3. ANÁLISIS GAP PARA LA NORMA ISO/IEC27001:2013

Se realiza un análisis deferencial con respecto a la norma ISO/IEC27001:2013 desarrollada para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI, aplica una estructura de alto nivel definidas en el anexo SL, en el que agrupa los requerimientos en siete clausulas.

De acuerdo a esto se valora cada una de los requisitos exigidos por la norma con base en entrevista al Responsable de TI y al Gerente General entendiendo que es una empresa que está iniciando su proceso de análisis de seguridad debido a las exigencias que han empezado a surgir en el mercado.

En la Tabla No. 3 se muestran el nivel de madurez obtenido de la situación actual de la empresa.

CLAUSULAS		VALORACIÓN	
4	Contexto de la organización	0,0%	No existe
5	Liderazgo	33,3%	Repetible
6	Planeación	0,0%	No existe
7	Soporte	0,0%	No existe
8	Operación	0,0%	No existe
9	Evaluación de rendimiento	0,0%	No existe
10	Mejora	0,0%	No existe
	PROMEDIO	**4,8%**	

Tabla No. 3: Niveles de madurez de la Empresa

La Figura No. 1 muestra la gráfica resultante expresando el estado en que se encuentra la empresa con respecto a los requisitos de la norma ISO/IEC27001:2013.

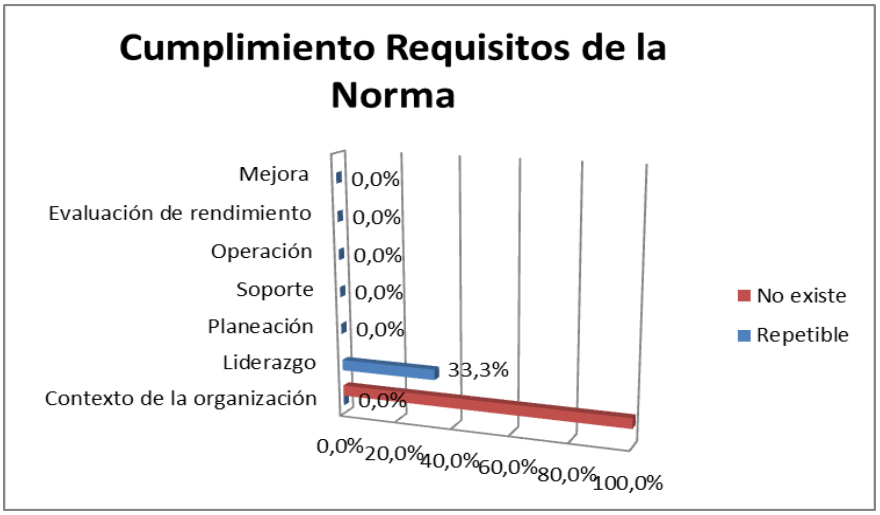

Gráfico No. 1: Cumplimiento Requisitos de la Norma ISO 27001:2013

De acuerdo a los resultados observados se puede determinar que la Empresa no evidencia el cumplimiento de los requisitos de la norma, aunque estén trabajando en estrategias para fortalecer la seguridad de la información. Además aunque se estén llevando a cabo algunos procedimientos asociados a la seguridad, no han sido documentados.

Esta falta de cumplimiento en seguridad en la organización, indica que la empresa se encuentra en un nivel de cumplimiento de tan solo 4,8% faltando 55,2 puntos porcentuales para alcanzar el nivel de madurez esperado.

NIVEL ALCANZADO	4,80%
NIVEL ESPERADO	60%

Tabla No. 4: Tabla Nivel de Cumplimiento General

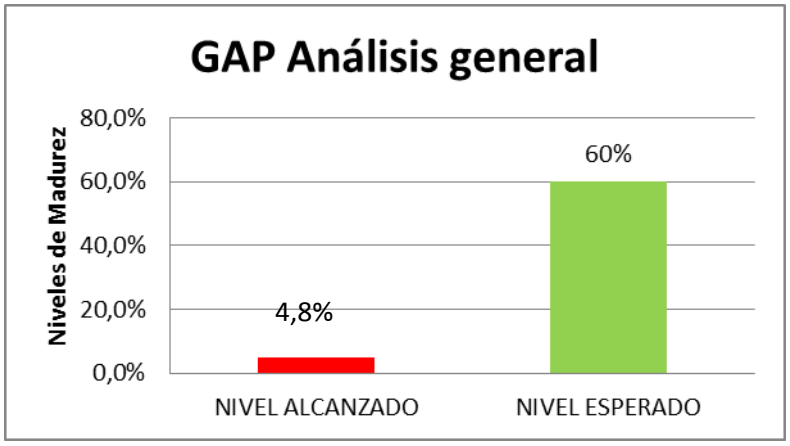

Gráfico No. 2: GAP Análisis General

4.4. ANÁLISIS GAP PARA LA NORMA ISO/IEC27002:2013

En la tabla No. 5 se describe el nivel de madurez que se obtuvo por cada dominio.

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO/IEC 27002:2013			
DOMINIOS DE CONTROL		**Porcentaje de Cumplimiento**	
5	Políticas de seguridad de la información	0%	No existe
6	Organización de la seguridad de la información	14%	Inicial
7	Seguridad delos recursos humanos	0%	No existe
8	Gestión de activos	10%	Inicial
9	Control de acceso	29%	Repetible
10	Criptografía	0%	No existe
11	Seguridad física y del entorno	29%	Repetible
12	Seguridad en las operaciones	0%	No existe
13	Seguridad de las comunicaciones	14%	Inicial
14	Adquisición, desarrollo y mantenimiento de sistemas	0%	No existe
15	Relaciones con los proveedores	0%	No existe
16	Gestión de incidentes en la seguridad de la información	0%	No existe
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0%	No existe
18	Cumplimiento	13%	Inicial

Tabla No. 5: Nivel de madurez Dominios de Control

Los aspectos detallados de las entrevistas realizadas por cada control se encuentran en el archivo:

ANÁLISIS GAP DETALLADO.xlsx

Para el diagnóstico de acuerdo a la norma ISO 27002:2013 de la Empresa, la Figura No. 3 muestra la gráfica resultante con respecto a los diferentes dominios establecidos en la norma.

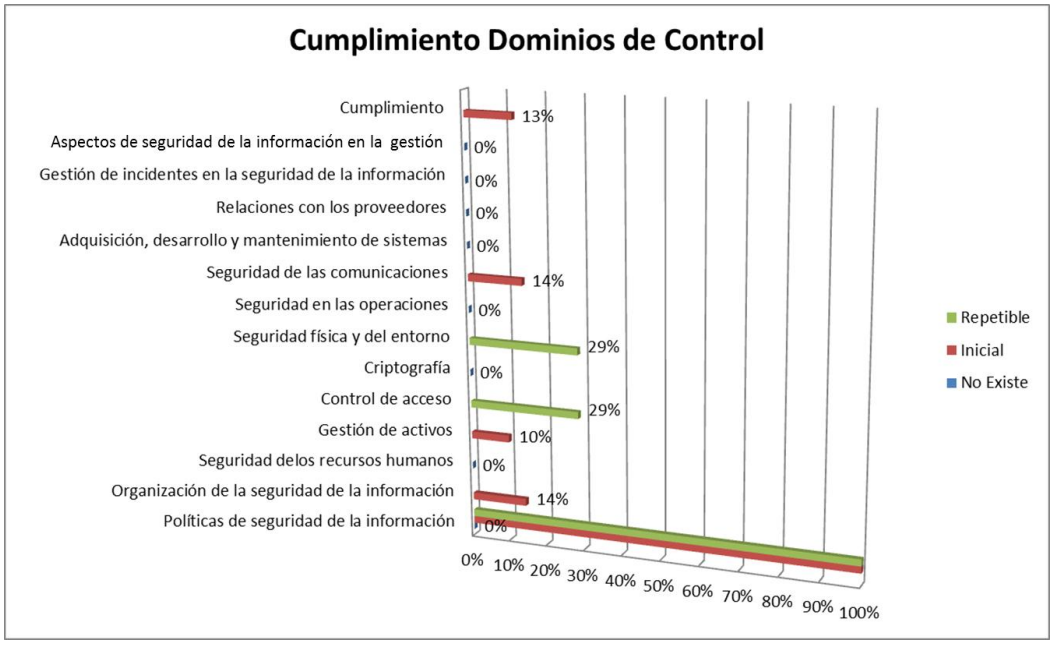

Gráfico No. 3: Cumplimiento Dominios de Control

De acuerdo a la situación actual se puede observar que la Empresa es consciente de su realidad y ha comenzado a establecer procedimientos para fortalecer los controles para mitigar los riesgos asociados a la seguridad lógica y física.

De la evaluación de los controles, el nivel de madurez indica que la mayor cantidad se encuentran en un estado de "No existe" e "Inicial" lo que define principalmente que:

- No se cuenta con un enfoque de administración de seguridad de la información y los pocos aspectos que se han iniciado se encuentran desorganizados.
- Ningún procedimientos asociados a la seguridad han sido documentado
- Existe un alto grado de confianza en el conocimiento del personal
- No hay comunicación formal de los eventos de seguridad

5. SISTEMA DE GESTIÓN DOCUMENTAL

5.1. INTRODUCCIÓN

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001.

5.2. ESQUEMA DOCUMENTAL

La norma ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el Sistema de Gestión de Seguridad de la Información. Estos documentos se describen a continuación:

- **Política de Seguridad:** Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe establecer aspectos globales a la seguridad de la información, definidos en el documento de "Política de Seguridad de la Información".

  Se incluye archivo:

  Anexo 1 - PSI-001_POLITICA_DE_SEGURIDAD DE LA INFORAMCION.pdf

- **Procedimiento de Auditorías Internas:** Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

  Se incluye archivo:

  Anexo 2 - PAI-002_PROCEDIMIENTO DE AUDITORIA.pdf

- **Gestión de Indicadores:** Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.

  Se incluye archivos:

  Anexo 3 - GIS-003_GESTION DE INDICADORES.pdf

  Anexo 4 - HVI-004_HOJA DE VIDA DE INDICADORES

- **Procedimiento Revisión por Dirección:** La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones

  Se incluye archivo:

  Anexo 5- PRD-005_PROCEDIMIENTO REVISION POR LA DIRECCION.pdf

- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

  Se incluye archivo:

  Anexo 6- GRR-006_GESTION DE ROLES Y RESPONSABILIDADES.pdf

- **Metodología de Análisis de Riesgos**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

  Se incluye archivo:

  Anexo 7- MAR-007_METODOLOGIA ANALISIS DE RIESGOS.pdf

- **Declaración de Aplicabilidad:** Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

  Se incluye archivo:

  Anexo 8 - DAC-008_DECLARACION DE APLICABILIDAD.pdf

5.3. RESULTADOS

Con el esquema documental básico que establece la norma preparada, tendremos establecidas las bases de nuestro Sistema de Gestión de Seguridad de la Información, ya que sobre estos documentos y/o políticas/procedimientos se llevarán a cabo las diferentes actividades de implantación (realización del análisis de riesgos, implantación de controles necesarios, implantación de proyectos, realización de auditoría interna, etc.).

6. ANÁLISIS DE RIESGO

6.1. INTRODUCCIÓN

Como ya es conocido los activos de información son de suma importancia para toda organización, debido a esto se requiere conocer los recursos de información con los que cuenta la organización, para de esta misma forma iniciar con la implementación del Plan de SGSI.

Magerit clasifica los activos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. Como primer paso para el Análisis de riesgos se realizará el Inventario de Activos y una clasificación de acuerdo al Tipo.

6.2. INVENTARIO DE ACTIVOS

Los activos se agruparán según sus características, valor y criticidad similares acordes con la metodología MAGERIT y se tendrá en cuenta las siguientes categorías:

GRUPO	ABREVIATURA	DESCRIPCIÓN
Instalaciones	[L]	Lugares donde se alojan los sistemas de información y comunicaciones.
Hardware	[HW]	Recursos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Aplicación	[SW]	Soporte lógico que permite gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios
Datos:	[D]	El activo que permite a la organización prestar sus servicios.
Redes de Comunicación	[COM]	Instalaciones dedicadas como servicios de comunicaciones para medios de transporte que llevan datos de un sitio a otro.
Servicios	[S]	Funciones que satisfacen las necesidad de los usuarios prestados por el sistema.
Equipamiento auxiliar	[AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Personal	[P]	Las personas relacionadas con los sistemas de información.

Tabla No. 6: Definición de Grupos de los activos

En la siguiente tabla se presentan los activos de información más importantes que actualmente posee la Empresa descritos en la **Tabla No. 1: Tabla de Recursos de Informáticos**:

ÁMBITO	ID	ACTIVO
Instalaciones [L]	[L-01]	Oficina de Sistemas
Hardware [HW]	[HW-01]	Servidor Principal
	[HW-02]	Servidor de Desarrollo y Pruebas
	[HW-03]	Desktop No. 1
	[HW-04]	Desktop No. 2
	[HW-05]	Desktop No. 3
	[HW-06]	Portátil

Aplicación [SW]	[SW-01]	Windows 7 Profesional
	[SW-02]	Windows 8.1
	[SW-03]	Microsoft Office
	[SW-04]	Antivirus
	[SW-05]	Windows Server 2008 R2
	[SW-06]	J2EE
	[SW-07]	MyEclipse IDE
	[SW-08]	Eclipse IDE for Java EE Developers
	[SW-09]	Aplicación Contable
	[SW-10]	Aplicación Micronif
	[SW-11]	Sigcoop 8.0
Datos[D]	[D-01]	Datos de Clientes, Asociados, Empleados.
	[D-02]	Códigos fuente.
	[D-03]	Datos de gestión Administrativa, contable y financiera.
	[D-04]	Copias de Seguridad
	[D-05]	Logs
Red de Comunicación [COM]	[COM-01]	ADSL Cable Modem
	[COM-02]	Rourter
	[COM-03]	Access Point
	[COM-04]	Red Telefónica
	[COM-05]	Red inalámbrica
Servicios [S]	[S-01]	Correo Electrónico
	[S-02]	Servicio Web
Equipamiento auxiliar [AUX]	[AUX-01]	Impresora s
	[AUX-02]	Regulador de Voltaje
	[AUX-03]	Aire Acondicionado
	[AUX-04]	Archivadores
Personal [P]	[P-01]	Responsable de TI
	[P-02]	Desarrolladores
	[P-03]	Demás personal de TI
	[P-04]	Personal de Administración
	[P-05]	Asociados

Tabla No. 7: Inventario de Activos

6.3. VALORACIÓN DE LOS ACTIVOS

La valoración de los activos se basó en el costo que representaría su reposición en caso de que se haya comprometido alguna de sus dimensiones de seguridad y las relaciones de dependencia que tienen con otros activos.

6.3.1. Análisis de dependencia de los Activos

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

Con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores.

En la figura No. 4 se presenta el Árbol de dependencia de activos de la empresa en estudio.

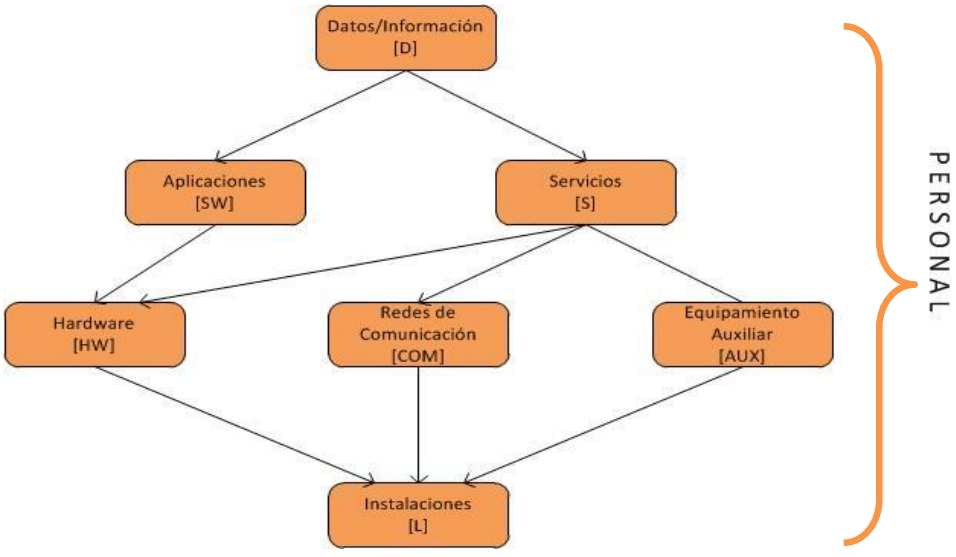

Figura No. 4: Árbol de Dependencias de Activos

En el Árbol de Dependencias podemos observar que en el nivel superior se ubica el tipo de activo más crítico, según los niveles establecidos por Magerit como esenciales se tiene para la empresa, La Información. También se observa que las Instalaciones no tienen dependencias y el Personal no se ubica como un nivel pues es transversa, a todos los niveles.

6.4. DIMENSIONES DE SEGURIDAD

La valoración de Activos se realizará teniendo en cuenta las dimensiones de: Confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad definidas en Magerit como:

- **Confiabilidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Disponibilidad**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
- **Trazabilidad**: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

A través de ellas se mostrará el impacto que las diferentes amenazas podrían causar a cada activo. En La tabla No. 3 del archivo (MAR-007_METODOLOGÍA ANALISIS DE RIESGOS) muestra los rangos de valoración.

Rango	valor		criterio
9 -10	muy alto	MA	daño muy grave
6-8	alto	A	daño grave
3-5	medio	M	daño importante
1-2	bajo	B	daño menor
0	Muy Bajo	MB	irrelevante a efectos prácticos

Tabla No. 3: Valoración Dimensiones de Seguridad

6.5. TABLA RESUMEN DE VALORACIÓN

En la tabla No. 8 se muestra la Valoración de los Activos y se complementa con una Valoración Cualitativa según criterios establecidos en la Metodología (MAR-007_METODOLOGÍA ANALISIS DE RIESGOS).

De la Figura No. 4: Árbol de Dependencias de Activos, se observa que la información se encuentra en un nivel esencial y en la Tabla No. 8: Valoración de Activos, el Código Fuente arroja un nivel de Importancia **Muy Alto**, ya que el Desarrollo de Software se ha convertido en el proceso con mayor fuerza en la Empresa Estudiada.

Para determinar la calificación cualitativa se utiliza la Tabla No. 4: Importancia de los Activos, de la Metodología Establecida.

valor	criterio	Rango
MA	muy alto	41-50
A	alto	26-40
M	medio	15-25
B	bajo	6-14
MB	Muy Bajo	0-5

Tabla No. 4: Importancia de los Activos

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS					TOTAL	IMPORTANCIA
			[A]	[C]	[I]	[D]	[T]		
Instalaciones [L]	[L-01]	Oficina de Sistemas	7	8	8	9	5	37	A
Hardware [HW]	[HW-01]	Servidores	5	9	9	8	6	37	A
	[HW-03]	Estaciones de Trabajo	3	2	1	1	1	8	B
Aplicación [SW]	[SW-01]	Sistemas Operativos	3	2	1	1	1	8	B
	[SW-03]	Microsoft Office	3	2	1	1	0	7	B
	[SW-04]	Antivirus	5	2	5	5	3	20	M
	[SW-05]	Windows Server 2008 R2	3	8	8	8	6	33	A
	[SW-07]	Herramientas de desarrollo	2	3	2	1	0	8	B
	[SW-09]	Aplicativo Contable	2	8	9	8	7	34	A
	[SW-10]	Aplicativo Micronif	5	9	5	5	3	27	A
	[SW-11]	Sigcoop 8.0	3	9	3	3	2	20	M
Datos[D]	[D-01]	Datos de Clientes, Asociados, Empleados.	6	7	9	3	7	32	A
	[D-02]	Códigos fuente.	7	9	9	8	8	41	MA
	[D-03]	Datos de gestión Administrativa, contable y financiera.	3	6	9	7	5	30	A
	[D-04]	Copias de Seguridad	4	10	10	6	5	35	A
	[D-05]	Logs	4	9	9	4	6	32	A
Red de Comunicación [COM]	[COM-01]	Dispositivos de Acceso a redes	3	8	9	3	7	30	A
	[COM-02]	Rourter	3	8	9	3	5	28	A
	[COM-04]	Red Telefónica	5	2	1	6	2	16	M
	[COM-05]	Red inalámbrica	4	7	9	7	5	32	A
Servicios [S]	[S-01]	Correo Electrónico	3	6	6	3	5	23	M
	[S-02]	Servicio Web	3	2	3	5	5	18	M
Equipamiento auxiliar [AUX]	[AUX-01]	Impresoras	0	0	0	1	0	1	MB
	[AUX-02]	Regulador de Voltaje	0	0	0	5	0	5	MB
	[AUX-03]	Aire Acondicionado	0	0	0	3	0	3	MB
	[AUX-04]	Archivadores	0	5	5	5	0	15	M

Personal [P]	[P-01]	Responsable de TI	2	2	2	8	5	19	M
	[P-02]	Desarrolladores	8	9	9	9	8	43	MA
	[P-03]	Demás personal de TI	0	0	0	2	0	2	MB
	[P-04]	Personal de Administración	0	0	0	2	2	4	MB
	[P-05]	Asociados	0	0	0	1	0	1	MB

Tabla No. 8: Valoración de Activos

6.6. ANÁLISIS DE AMENAZAS

Los activos se encuentran constantemente expuestos a amenazas de diferentes tipos que pueden reducir su uso y valor. Es necesario identificar dichas amenazas e indicar la frecuencia de ocurrencia, teniendo en cuenta que la materialización de dichas amenazas sobre el activo hará que su valor disminuya porcentualmente.

En la metodología del Análisis de Riesgos (MAR-007_METODOLOGIA ANALISIS DE RIESGOS.pdf) se define el tipo de amenazas que puede afectar los activos según su categoría, se toma como referencia la definición de Magerit.

La siguiente tabla muestra la valoración de las amenazas por dimensión:

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	1				100%	
[N.2]	Daños por agua	MP	1				70%	
[I.1]	Fuego	MP	1				100%	
[I.2]	Daños por agua	PF	0,1				50%	
[A.7]	Uso no previsto	N	1				20%	
[A.11]	Acceso no autorizado	PF	0,1		30%	30%		
[A.26]	Ataque destructivo	MP	0,01				100%	
Ámbito: Instalaciones	**Activo: [L-01] Oficina de Sistemas**	N	1,00	0,00	0,30	0,30	1,00	0,00

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	0,01				100%	
[N.2]	Daños por agua	MP	0,01				100%	
[I.1]	Fuego	MP	0,01				100%	
[I.2]	Daños por agua	PF	0,1				100%	
[I.3]	Contaminación mecánica	PF	0,1				50%	
[I.5]	Avería de origen físico o lógico	PF	0,1				50%	
[I.6]	Corte del suministro eléctrico	MP	0,01				50%	
[I.7]	Condiciones inadecuadas de temperatura o humedad	PF	0,1				100%	
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	PF	0,1				100%	
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50%	
[E.25]	Pérdida de equipos	PF	0,1		100%		100%	
[A.6]	Abuso de privilegios de acceso	N	1		100%		100%	
[A.7]	Uso no previsto	N	1		100%	30%	100%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.23]	Manipulación de los equipos	PF	0,1		50%	20%	50%	
[A.24]	Denegación de servicio	F	10				100%	
[A.25]	Robo	MP	0,01		100%		100%	
[A.26]	Ataque destructivo	MP	0,01				100%	
Ámbito: Hardware	**Activo: [HW-01] Servidor Principal [HW-02] Servidor de Desarrollo y Pruebas [HW-03] Estaciones de Trabajo No. 1, 2 y 3 [HW-06] Portátiles No. 1 y 2**	F	10,00	0,00	1,00	0,30	1,00	0,00

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.1]	Errores de los usuarios	´N	1		2%	2%	2%	
[E.2]	Errores de Administrador	PF	0,1		30%	20%	20%	
[E.8]	Difusión de software dañino	PF	0,1		5%	5%	5%	
[E.15]	Alteración accidental de la información	MF	100			20%		
[E.18]	Destrucción de información	N	1				30%	
[E.19]	Fugas de información	MF	100		50%			
[E.20]	Vulnerabilidades de los programas (software)	MF	100		50%	20%	5%	
[E.21]	Errores de mantenimiento / actualización de programas (software)	MF	100		1%	2%	2%	
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	100%	50%		
[A.6]	Abuso de privilegios de acceso	N	1		50%	20%	20%	
[A.7]	Uso no previsto	N	1		5%	5%	100%	
[A.8]	Difusión de software dañino	PF	0,1		100%	100%	100%	

[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.18]	Destrucción de información	PF	0,1				50%	
[A.19]	Divulgación de información	N	1		50%			
[A.22]	Manipulación de programas	PF	0,1		50%	50%	50%	
Ámbito: Aplicaciones	**Activo: [SW-01] Windows 7 Profesional [SW-02] Windows 8.1 [SW-03] Microsoft Office [SW-04] Antivirus [SW-05] Windows Server 2008 R2 [SW-06] J2EE [SW-07] MyEclipse IDE [SW-08] Eclipse IDE for Java EE Developers**	MF	100,00	1,00	1,00	1,00	1,00	0,00

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.1]	Errores de los usuarios	N	1		5%	5%	5%	
[E.2]	Errores de Administrador	PF	0,1		30%	20%	20%	
[E.8]	Difusión de software dañino	PF	0,1		5%	5%	5%	
[E.15]	Alteración accidental de la información	MF	100			20%		
[E.18]	Destrucción de información	N	1				30%	30%
[E.19]	Fugas de información	MF	100		50%			
[E.20]	Vulnerabilidades de los programas (software)	MF	100		50%	20%	5%	
[E.21]	Errores de mantenimiento / actualización de programas (software)	MF	100			1%	1%	
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	100%	50%		
[A.6]	Abuso de privilegios de acceso	N	1		50%	20%	20%	
[A.8]	Difusión de software dañino	PF	0,1		100%	100%	100%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.18]	Destrucción de información	PF	0,1				50%	
[A.19]	Divulgación de información	N	1		50%			
[A.22]	Manipulación de programas	PF	0,1		50%	50%	50%	
Ámbito: Aplicación-De Gestión	**Activo: [SW-09] Aplicativo Contable [SW-10] Aplicativo Micronif [SW-11] Sigcoop 8.0**	MF	100,00	100%	100%	100%	100%	30%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.1]	Errores de los usuarios	N	1			20%		
[E.2]	Errores de Administrador	PF	0,1		20%	30%	30%	
[E.4]	Errores de configuración (conf)	MF	100			20%	5%	
[E.14]	Escapes de información	F	10		50%			

[E.15]	Alteración accidental de la información	MF	100			30%		
[E.18]	Destrucción de información	N	1				50%	
[E.19]	Fugas de información	MF	100		30%			
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	50%	20%		
[A.6]	Abuso de privilegios de acceso	N	1		30%	5%		
[A.15]	Modificación deliberada de la información	N	1			30%		
[A.18]	Destrucción de información	PF	0,1				100%	
[A.19]	Divulgación de información	N	1		100%			
Ámbito: Datos	**Activo: [D-01] Datos de Clientes, Asociados, Empleados. [D-02] Códigos fuente. [D-03] Datos de gestión Administrativa, contable y financiera. [D-04] Copias de Seguridad**	MF	100,00	100%	100%	30%	100%	0%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.2]	Errores de Administrador	PF	0,1		5%	20%	5%	
[E.3]	Errores de monitorización	PF	0,1					50%
[E.4]	Errores de configuración (conf)	MF	100			20%		5%
[E.15]	Alteración accidental de la información	MF	100			5%		
[E.18]	Destrucción de información	N	1				100%	
[E.19]	Fugas de información	MF	100		30%			
[A.3]	Manipulación de los registros de actividad (log)	PF	0,1		20%	50%		50%
[A.4]	Manipulación de la configuración	PF	0,1	50%	50%	30%		5%
[A.13]	Repudio	PF	0,1					100%
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.18]	Destrucción de información	PF	0,1				50%	
[A.19]	Divulgación de información	N	1		50%			
Ámbito: Datos	**Activo: Logs**	MF	100,00	50%	50%	50%	100%	100%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.2]	Errores de Administrador	PF	0,1		20%	5%	50%	
[E.9]	Errores de reencaminamiento	PF	0,1		5%			
[E.10]	Errores de secuencia	PF	0,1			5%		
[E.14]	Escapes de información	MF	100		5%			
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50%	
[A.5]	Suplantación de la identidad del usuario	PF	0,1	50%	30%			
[A.6]	Abuso de privilegios de acceso	N	1			30%		
[A.7]	Uso no previsto	N	1		5%	5%	50%	

[A.9]	Reencaminamiento de mensajes	PF	0,1		5%			
[A.10]	Alteración de secuencia	PF	0,1			5%		
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.12]	Análisis de tráfico	PF	0,1		30%			
[A.14]	Interceptación de información (escucha)	PF	0,1		50%			
[A.24]	Denegación de servicio	F	10				50%	
Ámbito: Red de Comunicación	**Activo: [COM-01] ADSL Cable Modem [COM-02] Rourter [COM-03] Access Point [COM-04] Red Telefónica [COM-05] Red inalámbrica**	MF	100,00	50%	50%	30%	50%	0%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.1]	Errores de los usuarios	N	1		5%	2%	2%	
[E.2]	Errores de Administrador	PF	0,1		5%	20%	20%	
[E.15]	Alteración accidental de la información	MF	100			5%		
[E.18]	Destrucción de información	N	1				100%	
[E.19]	Fugas de información	MF	100		20%			
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	50%	20%		
[A.6]	Abuso de privilegios de acceso	N	1		20%	50%	20%	
[A.7]	Uso no previsto	N	1		5%	5%	50%	
[A.8]	Difusión de software dañino	PF	0,1		50%	50%	50%	
[A.10]	Acceso no autorizado	PF	0,1		30%	30%		
[A.13]	Repudio	PF	0,1					100%
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.19]	Divulgación de información	N	1		100%			
[A.24]	Denegación de servicio	F	10				100%	
Ámbito: Servicios	**Activo: [S-01] Correo Electrónico [S-02] Servicio Web**	MF	100,00	100%	100%	50%	100%	100%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	0,01				100%	
[N.2]	Daños por agua	MP	0,01				100%	
[I.1]	Fuego	MP	0,01				100%	
[I.2]	Daños por agua	PF	0,1				100%	
[I.3]	Contaminación mecánica	PF	0,1				50%	
[I.5]	Avería de origen físico o lógico	PF	0,1				50%	
[I.6]	Corte del suministro eléctrico	N	1				50%	
[E.25]	Pérdida de equipos	PF	0,1				100%	
[A.7]	Uso no previsto	N	1				50%	
[A.11]	Acceso no autorizado	PF	0,1		5%	5%		
[A.25]	robo	MP	0,01				100%	
[A.26]	Ataque destructivo	MP	0,01				100%	

Ámbito: Equipamiento auxiliar	**Activo: [AUX-01] Impresoras [AUX-02] Regulador de Voltaje [AUX-03] Aire Acondicionado**	N	1,00	0%	5%	5%	100%	0%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	0,01				100%	
[N.2]	Daños por agua	MP	0,01				100%	
[I.1]	Fuego	MP	0,01				100%	
[I.2]	Daños por agua	PF	0,1				100%	
[I.5]	Avería de origen físico o lógico	PF	0,1				20%	
[E.25]	Pérdida de equipos	PF	0,1				20%	
[A.7]	Uso no previsto	N	1		5%	5%	50%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.25]	robo	MP	0,01				100%	
[A.26]	Ataque destructivo	MP	0,01				100%	
Ámbito: Equipamiento auxiliar	**Activo: [AUX-01] Archivadores**	N	1,00	0%	50%	30%	100%	0%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.7]	Deficiencias y fallos en la organización	F	10				5%	
[E.19]	Fugas de información	MF	100		20%			
[E.28]	Indisponibilidad del personal	N	1				100%	
[A.29]	Extorsión	MP	0,01		5%	5%	5%	
[A.30]	Ingeniería social	MP	0,01		5%	5%	5%	
Ámbito: Personal	**Activo: [P-01] Responsable de TI [P-02] Desarrolladores [P-03] Demás personal de TI [P-04] Personal de Administración [P-05] Asociados**	MF	100,00	0%	20%	5%	100%	0%

Tabla No. 9: Valoración de Amenazas

6.7. IMPACTO POTENCIAL

Una vez obtenida los valores de los diferentes activos y la tabla de valoración de amenazas, se determina el impacto potencial que ocasionaría la materialización de dichas amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen los controles.

La siguiente tabla muestra la valoración del Impacto Potencial por cada dimensión con base en el valor del Activo y el valor de la Amenaza:

ID	ACTIVO	VALORACIÓN ACTIVOS					IMPORTANCIA	VALORACIÓN AMENAZAS					IMPACTO POTENCIAL				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas	7	8	8	9	5	A	0%	30%	30%	100%	0%	0	2,4	2,4	9	0
[HW-01]	Servidor Principal	5	9	9	8	6	A	0%	100%	30%	100%	0%	0	9	2,7	8	0
[HW-02]	Servidor de Desarrollo y Pruebas	3	5	5	5	2	M	0%	100%	30%	100%	0%	0	5	1,5	5	0
[HW-03]	Estaciones de Trabajo No. 1, 2 y 3	3	2	1	1	1	B	0%	100%	30%	100%	0%	0	2	0,3	1	0
[HW-06]	Portátiles No. 1 y 2	3	2	1	1	1	B	0%	100%	30%	100%	0%	0	2	0,3	1	0
[SW-01]	Windows 7 Profesional	3	2	1	1	1	B	100%	100%	100%	100%	0%	3	2	1	1	0
[SW-02]	Windows 8.1	3	2	1	1	1	B	100%	100%	100%	100%	0%	3	2	1	1	0
[SW-03]	Microsoft Office	3	2	1	1	0	B	100%	100%	100%	100%	0%	3	2	1	1	0
[SW-04]	Antivirus	5	2	5	5	3	M	100%	100%	100%	100%	0%	5	2	5	5	0
[SW-05]	Windows Server 2008 R2	3	8	8	8	6	A	100%	100%	100%	100%	0%	3	8	8	8	0
[SW-06]	J2EE	2	3	2	1	0	B	100%	100%	100%	100%	0%	2	3	2	1	0
[SW-07]	MyEclipse IDE	2	3	2	1	0	B	100%	100%	100%	100%	0%	2	3	2	1	0
[SW-08]	Eclipse IDE for Java EE Developers	2	3	2	1	0	B	100%	100%	100%	100%	0%	2	3	2	1	0
[SW-09]	Aplicativo Contable	2	8	9	8	7	A	100%	100%	100%	100%	30%	2	8	9	8	2,1
[SW-10]	Aplicativo Micronif	5	9	5	5	3	A	100%	100%	100%	100%	30%	5	9	5	5	0,9
[SW-11]	Sigcoop 8.0	3	9	3	3	2	M	100%	100%	100%	100%	30%	3	9	3	3	0,6
[D-01]	Datos de Clientes, Asociados, Empleados.	6	7	9	3	7	A	100%	100%	30%	100%	0%	6	7	2,7	3	0
[D-02]	Códigos fuente.	7	9	9	8	8	MA	100%	100%	30%	100%	0%	7	9	2,7	8	0
[D-03]	Datos de gestión Administrativa, contable y financiera.	3	6	9	7	5	A	100%	100%	30%	100%	0%	3	6	2,7	7	0
[D-04]	Copias de Seguridad	4	10	10	6	5	A	100%	100%	30%	100%	0%	4	10	3	6	0
[D-05]	Logs	4	9	9	4	6	A	50%	50%	50%	100%	100%	2	4,5	4,5	4	6
[COM-01]	ADSL Cable Modem	3	8	9	3	7	A	50%	50%	30%	50%	0%	1,5	4	2,7	1,5	0
[COM-02]	Rourter	3	8	9	3	5	A	50%	50%	30%	50%	0%	1,5	4	2,7	1,5	0
[COM-03]	Access Point	4	8	9	3	6	A	50%	50%	30%	50%	0%	2	4	2,7	1,5	0
[COM-	Red Telefónica	5	2	1	6	2	M	50%	50%	30%	50%	0%	2,5	1	0,3	3	0

04]																	
[COM-05]	Red inalámbrica	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[S-01]	Correo Electrónico	3	6	6	3	5	M	100%	100%	50%	100%	100%	3	6	3	3	5
[S-02]	Servicio Web	3	2	3	5	5	M	100%	100%	50%	100%	100%	3	2	1,5	5	5
[AUX-01]	Impresoras	0	0	0	1	0	MB	0%	5%	5%	100%	0%	0	0	0	1	0
[AUX-02]	Regulador de Voltaje	0	0	0	5	0	MB	0%	5%	5%	100%	0%	0	0	0	5	0
[AUX-03]	Aire Acondicionado	0	0	0	3	0	MB	0%	5%	5%	100%	0%	0	0	0	3	0
[AUX-04]	Archivadores	0	5	5	5	0	M	0%	50%	30%	100%	0%	0	2,5	1,5	5	0
[P-01]	Responsable de TI	2	2	2	8	5	M	0%	20%	5%	100%	0%	0	0,4	0,1	8	0
[P-02]	Desarrolladores	8	9	9	9	8	MA	0%	20%	5%	100%	0%	0	1,8	0,5	9	0
[P-03]	Demás personal de TI	0	0	0	2	0	MB	0%	20%	5%	100%	0%	0	0	0	2	0
[P-04]	Personal de Administración	0	0	0	2	2	MB	0%	20%	5%	100%	0%	0	0	0	2	0
[P-05]	Asociados	0	0	0	1	0	MB	0%	20%	5%	100%	0%	0	0	0	1	0

Tabla No. 10: Impacto Potencial

6.8. NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Una vez calculado el nivel del Impacto Potencial por cada activo, de igual forma se deberá calcular el nivel del riesgo al cual se encuentra sometida la Empresa. De esta manera se podrá definir si se implementan controles o no, estableciendo un nivel de riesgo aceptable, de tal manera que se puedan designar recursos para implementar controles que ayuden a minimizar los riegos sobre los activos que superen los niveles de riesgo aceptable.

Este nivel de riesgo aceptable tiene que estar aprobado por la Alta Dirección, y se tienen que definir los criterios para establecer dicho nivel.

Este cálculo del Riesgo total se obtendrá con la siguiente formula:

Riesgo = impacto potencial x frecuencia

ID	ACTIVO	FRECUENCIA		IMPACTO POTENCIAL					RIESGO				
				[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas	N	1	0	2,4	2,4	9	0	0,00	2,40	2,40	9	0,00
[HW-01]	Servidor Principal	F	10	0	9	2,7	8	0	0,00	90	27	80	0,00
[HW-02]	Servidor de Desarrollo y Pruebas	F	10	0	5	1,5	5	0	0,00	50	15	50	0,00
[HW-03]	Estaciones de Trabajo No. 1, 2 y 3	F	10	0	2	0,3	1	0	0,00	20	3	10	0,00
[HW-06]	Portátiles No. 1 y 2	F	10	0	2	0,3	1	0	0,00	20	3	10	0,00
[SW-01]	Windows 7 Profesional	MF	100	3	2	1	1	0	300	200	100	100	0,00
[SW-02]	Windows 8.1	MF	100	3	2	1	1	0	300	200	100	100	0,00
[SW-03]	Microsoft Office	MF	100	3	2	1	1	0	300	200	100	100	0,00
[SW-04]	Antivirus	MF	100	5	2	5	5	0	500	200	500	500	0,00
[SW-05]	Windows Server 2008 R2	MF	100	3	8	8	8	0	300	800	800	800	0,00
[SW-06]	J2EE	MF	100	2	3	2	1	0	200	300	200	100	0,00
[SW-07]	MyEclipse IDE	MF	100	2	3	2	1	0	200	300	200	100	0,00
[SW-08]	Eclipse IDE for Java EE Developers	MF	100	2	3	2	1	0	200	300	200	100	0,00
[SW-09]	Aplicativo Contable	MF	100	2	8	9	8	2,1	200	800	900	800	210
[SW-10]	Aplicativo Micronif	MF	100	5	9	5	5	0,9	500	900	500	500	90
[SW-11]	Sigcoop 8.0	MF	100	3	9	3	3	0,6	300	900	300	300	60
[D-01]	Datos de Clientes, Asociados, Empleados.	MF	100	6	7	2,7	3	0	600	700	270	300	0,00
[D-02]	Códigos fuente.	MF	100	7	9	2,7	8	0	700	900	270	800	0,00
[D-03]	Datos de gestión Administrativa, contable y financiera.	MF	100	3	6	2,7	7	0	300	600	270	700	0,00
[D-04]	Copias de Seguridad	MF	100	4	10	3	6	0	400	1.000	300	600	0,00
[D-05]	Logs	MF	100	2	4,5	4,5	4	6	200	450	450	400	600
[COM-01]	ADSL Cable Modem	MF	100	1,5	4	2,7	1,5	0	150	400	270	150	0,00

[COM-02]	Rourter	MF	100	1,5	4	2,7	1,5	0	150	400	270	150	0,00
[COM-03]	Access Point	MF	100	2	4	2,7	1,5	0	200	400	270	150	0,00
[COM-04]	Red Telefónica	MF	100	2,5	1	0,3	3	0	250	100	30	300	0,00
[COM-05]	Red inalámbrica	MF	100	2	3,5	2,7	3,5	0	200	350	270	350	0,00
[S-01]	Correo Electrónico	MF	100	3	6	3	3	5	300	600	300	300	500
[S-02]	Servicio Web	MF	100	3	2	1,5	5	5	300	200	150	500	500
[AUX-01]	Impresoras	N	1	0	0	0	1	0	0,00	0,00	0,00	1	0,00
[AUX-02]	Regulador de Voltaje	N	1	0	0	0	5	0	0,00	0,00	0,00	5	0,00
[AUX-03]	Aire Acondicionado	N	1	0	0	0	3	0	0,00	0,00	0,00	3	0,00
[AUX-04]	Archivadores	N	1	0	2,5	1,5	5	0	0,00	2,50	1,50	5	0,00
[P-01]	Responsable de TI	MF	100	0	0,4	0,1	8	0	0,00	40	10	800	0,00
[P-02]	Desarrolladores	MF	100	0	1,8	0,45	9	0	0,00	180	45	900	0,00
[P-03]	Demás personal de TI	MF	100	0	0	0	2	0	0,00	0,00	0,00	200	0,00
[P-04]	Personal de Administración	MF	100	0	0	0	2	0	0,00	0,00	0,00	200	0,00
[P-05]	Asociados	MF	100	0	0	0	1	0	0,00	0,00	0,00	100	0,00

Tabla No. 11: Valoración de Riesgos

6.8.1. Selección de Controles

Considerando que hasta el momento en la empresa no se ha llevado a cabo un proceso formal de implementación de controles para el ambiente de TI, se iniciará en este aparte la selección de Controles de acuerdo al resultado de los riesgos determinados y que aparecen en el cuadro anterior. Para ello se ha tenido en cuenta los grupos de activos que se definieron por cada una de sus dimensiones y el riesgo que generaron. Se utilizan controles proporcionados por la Norma ISO/IEC 27002.

Esta selección se encuentra en el archivo:
Anexo 9 - SCC-009_SELECCION CONTROLES.pdf

6.8.2. Riesgo Aceptable y Riesgo Residual

La Alta Dirección establece que el nivel de riesgo aceptable es 100, que corresponde al Nivel Medio, por lo tanto todo lo que esté por debajo de este nivel, se considerará como una amenaza no importante para la empresa, que no será incluida para la asignación de controles y serán tratados como riesgos residuales. Todo valor superior a éste indica que se debe establecer controles que mitiguen el riesgo asociado. La aprobación de estos criterios encuentra en el documento:

Anexo 10 - AAD-010_APROBACION ALTA DIRECCION.pdf

Posteriormente de acuerdo a la criticidad de los riesgos sobre los activos se asignaran los controles que presenten mayor urgencia.

6.9. RESULTADOS

Una vez realizadas las tareas contempladas en esta fase, se llega a los siguientes resultados:

- Análisis detallado de los activos relevantes a nivel de seguridad para la empresa.

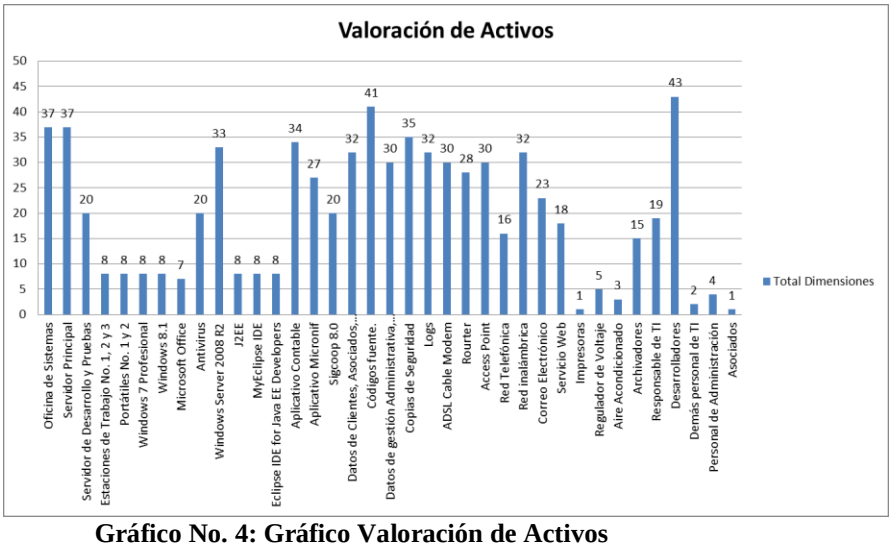

Gráfico No. 4: Gráfico Valoración de Activos

Como se observa en la Gráfica No. 4, tomando como base el total de las 5 dimensiones, los Desarrolladores, Códigos Fuente, Oficina de Sistemas y Servidores son activos con los valores más altos, lo que supone una gestión prioritaria considerando que la empresa no ha estimado controles adecuados para su protección.

- Estudio de posibles amenazas sobre los sistemas de información y su impacto

En los grupos de activos de acuerdo a las amenazas comunes se globalizan la frecuencia, observándose que, aunque la empresa presenta algunos controles básicos la mayoría muestran una frecuencia alta, en especial en amenazas que comprometen la confidencialidad de la información, tales como:

  - Alteración accidental de la información
  - Fugas de información
  - Vulnerabilidades de los programas (software)
  - Errores de mantenimiento / actualización de programas (software)
  - Errores de configuración (conf)

- Evaluación del impacto potencial que tendría la materialización de las diferentes amenazas a que están expuestas nuestros activos.

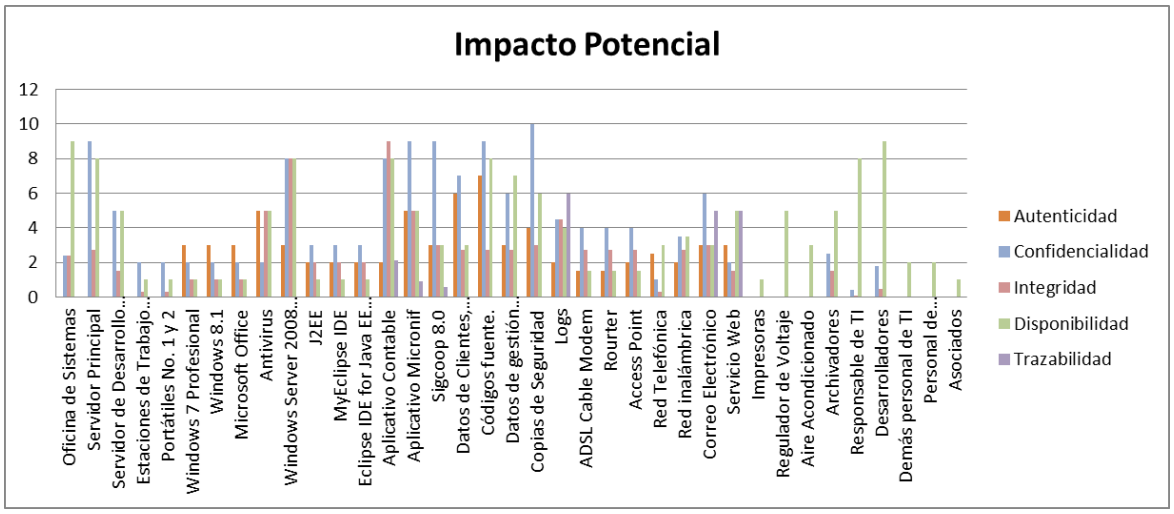

Gráfico No. 5: Gráfico Impacto Potencial

Se evidencia que la dimensión de disponibilidad con respecto a la mayoría de los activos, en especial las copias de seguridad, los códigos fuente y los servidores presentan alto impacto con la materialización de las amenazas. Estos activos son básicos para la continuidad del negocio y recuperación de desastres.

De otro lado la dimensión confidencialidad puede tener como consecuencia pérdida de imagen de la organización.

- Evaluación de los Riesgos

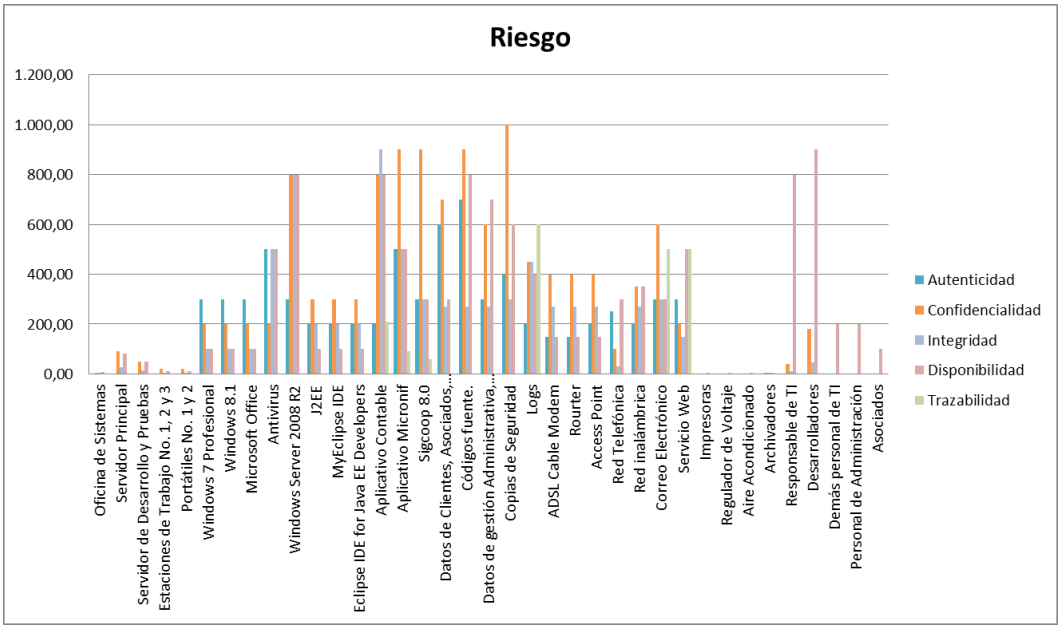

Gráfico No. 6: Riesgos

Las amenazas mencionadas anteriormente también tipifican riesgos especialmente relacionados con la confidencialidad de la información como lo muestra la Grafica No.6 denotando una implementación de controles con mayor urgencia en activos como:

- Copias de seguridad
- Código fuente
- Aplicativos

- Y Software de Servidores

7. PROPUESTAS DE PROYECTOS

7.1. INTRODUCCIÓN

Una vez realizado el análisis de riesgos es conocido el nivel de exposición en que se encuentra la organización, para ello se plantea diferentes propuestas de mejora que ayuden a mitigar el riesgo actual, de igual forma se pretende dar cumplimiento en mayor parte a los requisitos de la norma.

El Plan de Seguridad planteado incidirá en la mejora relacionada con la gestión de la seguridad y también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

7.2. PLAN DE SEGURIDAD

Siguiendo la metodología de Magerit (Libro I: Método, capítulo 6) a continuación se plantea el Plan de Seguridad (PS), en el que se identifican 3 tareas:

PS.1 – Identificación de proyectos de seguridad
PS.2 – Plan de ejecución
PS.3 – Ejecución (Esta etapa la llevará a cabo la empresa)

7.2.1. Identificación de proyectos de seguridad

Los proyectos planteados serán un conjunto de recomendaciones resultado de la fase de análisis de riesgos, para facilitar su ejecución. Estos deberán ayudar a minimizar el riesgo

actual en la organización y dar evolución al cumplimiento de la norma hasta un nivel adecuado.

En la tabla No. 12 se presenta una relación de proyectos por dominio:

PROYECTOS POR DOMINIOS DE CONTROL		
5		**Políticas de seguridad de la información**
	PS-010	Políticas de seguridad de la información
6		**Organización de la seguridad de la información**
	PS-011	Organización de la seguridad de la información
7		**Seguridad delos recursos humanos**
	PS-009	Continuidad del SGSI ante la ausencia de personal relacionado
	PS-008	**Continuidad de los procesos ante la ausencia de personal**
8		**Gestión de activos**
	PS-001	Legalización y controles de Software de Infraestructura y de Gestión
	PS-012	Gestión de los activos
9		**Control de acceso**
	PS-001	Legalización y controles de Software de Infraestructura y de Gestión
	PS-002	Gestión de privilegios y Acceso a los aplicativos
10		**Criptografía**
11		**Seguridad física y del entorno**
	PS-013	Sistema de control de acceso físico
	PS-014	Sistema de control fisico de los equipos
12		**Seguridad en las operaciones**
	PS-001	Legalización y controles de Software de Infraestructura y de Gestión
	PS-002	Gestión de privilegios y Acceso a los aplicativos
	PS-003	Mejoramiento en el proceso de copias de seguridad
	PS-004	Gestión de logs
13		**Seguridad de las comunicaciones**
	PS-006	Garantizar la continuidad del servicio en caso de caida de las redes
	PS-007	Mejoramiento en el Servicio de Correos
14		**Adquisición, desarrollo y mantenimiento de sistemas**
	PS-002	Gestión de privilegios y Acceso a los aplicativos
15		**Relaciones con los proveedores**
	PS-015	Políticas de relación con los proveedores
16		**Gestión de incidentes en la seguridad de la información**
	PS-016	Políticas de incidentes de seguridad de la información
17		**Aspectos de seguridad de la información en la gestión de continuidad de negocio**

	PS-005	Garantizar la continuidad del servicio en caso de no disponibilidad de equipos de comunicaciones
	PS-006	Garantizar la continuidad del servicio en caso de caida de las redes
	PS-019	Plan de continuidad de negocio
18		**Cumplimiento**
	PS-001	Legalización y controles de Software de Infraestructura y de Gestión
	PS-017	Cumplimiento de normativa legal y de la organización
	PS-018	Cumplimiento de auditorías al SGSI

Tabla No. 12: Proyectos por Dominio de Control

7.2.2. Plan de ejecución

Continuando con la metodología para dar ejecución a cada uno de los proyectos planteados, se deberá tener en cuenta los siguientes factores:

- La criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas.
- El costo del programa.
- La disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas.
- Otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual entre otros.

El detalle de los proyectos para mejorar la seguridad de la información de la empresa se presenta en el archivo:
Anexo 11 - EDP-011_ESPECIFICACION DE PROYECTOS.xlsx

7.2.3. Cronograma

La ejecución de todos los proyectos del plan de seguridad se llevará a cabo en un periodo de 3 años, su ejecución durante el periodo planificado aparece en la tabla No. 12.

CODIGO	PROYECTO	TIEMPO EN MESES	AÑO 1 2016	AÑO 2 2017	AÑO 3 2018
PS-010	Política de seguridad de la información	2			
PS-004	Gestión de logs	1			
PS-003	Mejoramiento en el proceso de copias de seguridad	3			
PS-001	Legalización y controles de Software de Infraestructura	5			
PS-012	Clasificación de la informació	1			
PS-011	Organización de la seguridad de la información	2			
PS-013	Sistema de control de acceso	2			
PS-002	Gestión de privilegios y Acceso a los aplicativos	2			
PS-006	Garantizar la continuidad del servicio en caso de caida de las redes	1			
PS-017	Cumplimiento de normativa	2			
PS-007	Mejoramiento en el Servicio de Correos	2			
PS-008	Continuidad de los procesos ante la ausencia de personal	2			
PS-005	Garantizar la continuidad del servicio en caso de no disponibilidad de equipos de comunicaciones	3			
PS-009	Continuidad del SGSI ante la ausencia de personal relacionado	2			
PS-014	Sistema de control fisico de los equipos	1			
PS-015	Políticas de relación con los proveedores	1			
PS-016	Políticas de incidentes de seguridad de la información	1			
PS-018	Cumplimiento de auditorías al SGSI	2			
PS-019	Plan de continuidad de negocio	3			

Tabla No. 13: Cronograma

7.2.4. Presupuesto

Los recursos y presupuesto detallados de cada uno de los proyectos, teniendo en cuenta los recursos de hardware, software y número de horas hombre, se muestran en el archivo:

A continuación se presenta el resumen del presupuesto de los proyectos por los 3 años:

RESUMEN PRESUPUESTO POR AÑO		
Año	**Proyectos**	**Presupuesto**
Año 1	PS-001	$ 7.500.000
	PS-003	$ 1.900.000
	PS-004	$ 720.000
	PS-010	$ 1.800.000
	PS-12	$ 1.500.000
Total		**$ 13.420.000**
Año 2	PS-011	$ 1.800.000
	PS-013	$ 1.500.000
	PS-002	$ 1.200.000
	S-006	$ 900.000
	PS-017	$ 900.000
	PS-007	$ 900.000
	PS-008	$ 1.500.000
Total		**$ 8.700.000**
Año 3	PS-005	$ 4.800.000
	PS-009	$ 1.500.000
	PS-014	$ 720.000
	PS-015	$ 720.000
	PS-016	$ 720.000
	PS-018	$ 1.500.000
	PS-019	$ 1.800.000
Total		**$ 11.760.000**
Gran Total		**$ 33.880.000**

Tabla No. 14: Presupuesto Resumen por año

7.3. RESULTADOS

7.3.1. Nivel cumplimiento de los requisitos de la norma ISO/IEC 27002:2013

En la tabla No. 15 se muestra, una línea base que representa el resultado inicial obtenido en el análisis GAP de cada uno de los dominios, las metas de evolución esperadas a 3 años con la implementación de cada uno de los proyectos y una simulación de los progresos por cada periodo, con estas variable y en tiempo se puede ir midiendo la evolución de cada dominio.

El cálculo de los resultados se detalla a continuación:

Progreso_año = (Vr. progreso – Vr. actual) / (Vr. meta - Vr. actual)

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO/IEC 27002:2013											
DOMINIOS DE CONTROL		Progreso 2016	Progreso 2017	Progreso 2018	Valor observado 2016	Valor observado 2017	Valor observado 2018	Linea Base	METAS		
									2016	2017	2018
5	Políticas de seguridad de la información	60%	0%	0%	60	0	0	0%	100	100	100
6	Organización de la seguridad de la información	86%	78%	100%	12	35	60	14%	14	45	60
7	Seguridad delos recursos humanos	0%	88%	92%	0	35	55	0%	0	40	60
8	Gestión de activos	50%	100%	100%	20	60	60	10%	40	60	60
9	Control de acceso	0%	0%	92%	0,4	0,4	55	29%	29	29	60
10	Criptografía	0%	0%	0%	0	0	0	0%	0	0	0
11	**Seguridad física y del entorno**	0%	66%	83%	0	30	50	29%	29	45	60
12	Seguridad en las operaciones	33%	100%	92%	10	60	55	0%	30	60	60
13	Seguridad de las comunicaciones	0%	100%	92%	0	60	55	14%	14	60	60
14	Adquisición, desarrollo y mantenimiento de sistemas	0%	100%	100%	0	60	60	0%	0	60	60
15	**Relaciones con los proveedores**	0%	0%	83%	0	0	50	0%	0	0	60
16	Gestión de incidentes en la seguridad de la información	0%	0%	75%	0	0	45	0%	0	0	60
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0%	50%	92%	0	15	55	0%	0	30	60
18	Cumplimiento	50%	90%	100%	15	45	60	13%	30	50	60

Tabla No. 15: Nivel de cumplimiento de los Requisitos

Posteriormente, se representa mediante el siguiente gráfico la evolución del cumplimiento de los requisitos de la norma ISO/IEC 27002:2013 según la planificación realizada durante los 3 años del plan:

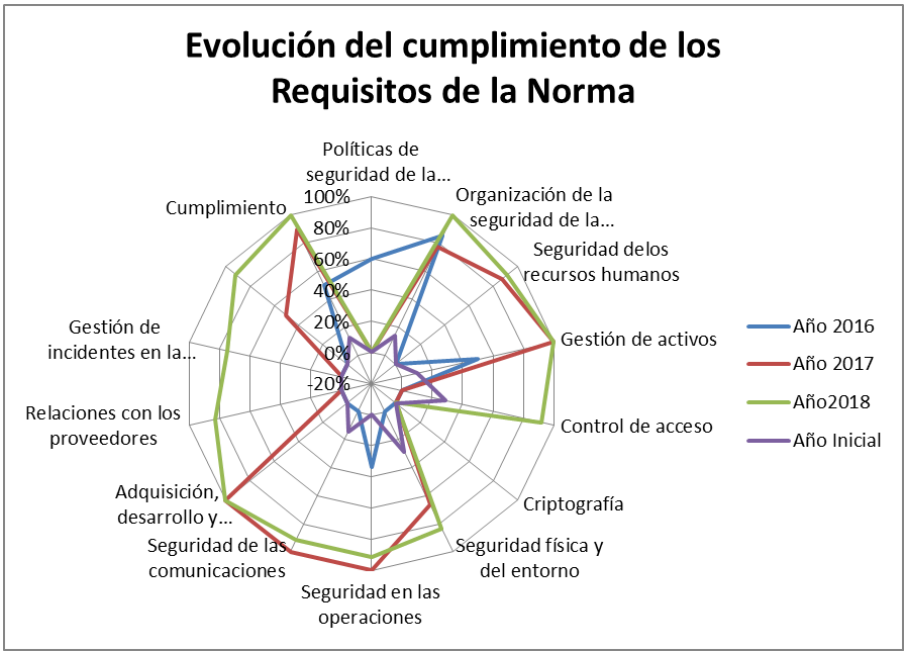

Gráfico No. 7: Evolución del cumplimiento de los Requisitos de la Norma

Como se puede observar en el Año Inicial se ve la total ausencia de aspectos de seguridad en los dominios 5, 7, 10, 14, 15 y 16. Y en los otros dominios unos valores muy bajos, por lo que es necesario tomar medidas prioritarias para resolverlos.

Con los proyectos que se planea implementar en el primer año, se pretende subsanar aspectos que son bastante delicados y que ante un eventual incidente puede ocasionar gran perjuicio a la empresa, como es la legalización del software y mejorar los procesos de copias de seguridad. También con la Política de Seguridad y la Gestión de Logs se deja en gran medida mejorado el año inicial para los años siguientes.

8. AUDITORÍA DE CUMPLIMIENTO

8.1. INTRODUCCIÓN

Iniciando con la identificación de los activos y la posterior evaluación de las amenazas, se ha logrado identificar los riesgos a los que se expone la empresa, de igual forma se establecieron controles con el propósito de reducir el impacto de estas amenazas. Por lo tanto es procedente realizar una evaluación a la empresa para determinar el grado de cumplimiento de los controles en cuanto a la seguridad de la información, establecidos en la norma ISO/IEC 27002:2013.

8.2. METODOLOGÍA

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad de la información en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Cuya estimación se realizará según el Modelo de Madurez de la Capacidad (CMM):

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	Reprodducible, 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.
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 No. 16: Modelo de Madurez de la Capacidad CMM

8.3. EVALUACIÓN DE LA MADUREZ

El estudio del cumplimiento de cada uno de los controles de los diferentes dominios de la ISO/IEC 27002, se encuentran en el archivo:

Anexo 12 - MMD-012_MODELO DE MADUREZ CMM.pdf.

8.4. PRESENTACIÓN DE RESULTADOS

8.4.1. Nivel de madurez porcentual por número de controles

Haciendo un resumen del resultado del nivel de madurez de los controles por cada dominio, la gráfica No. 8, muestra los siguientes los resultados:

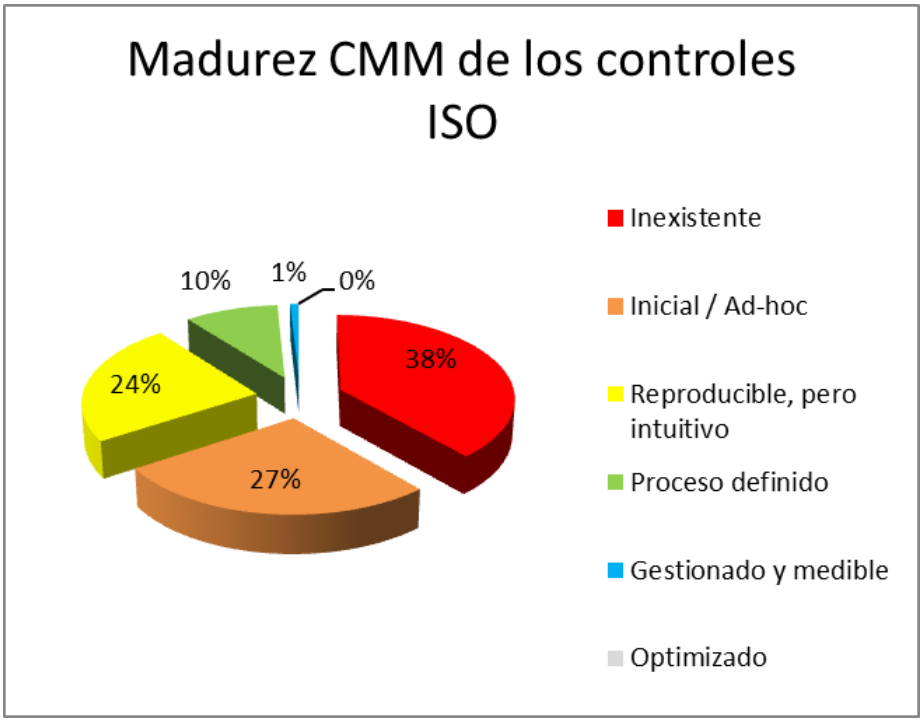

Gráfico No. 8: Madurez CMM de los controles ISO 27002:2013

En la gráfica se puede observar que aun cuando para la mayoría de los controles se desarrollaron proyectos, la empresa presenta un nivel de madurez en sus procesos de seguridad inexistente en un 38%, en un nivel inicial (27%), reproducible en un 24% y solamente un 10% de procesos definidos.

La mejora en el nivel de madurez reproducible se refleja en que algunos procedimientos y formatos han sido definidos, pero la mayoría de ellos no han sido formalizados ni comunicado al personal, como tampoco son suficientes para cubrir todo el sistema.

No se ha logrado cumplir con el total de los proyectos planeados y de los requisitos esperados. Los asociados son conscientes de la importancia de los proyectos, pero aun las actividades se realizan por esfuerzos personales.

8.4.2. Nivel de Cumplimiento por Dominio ISO

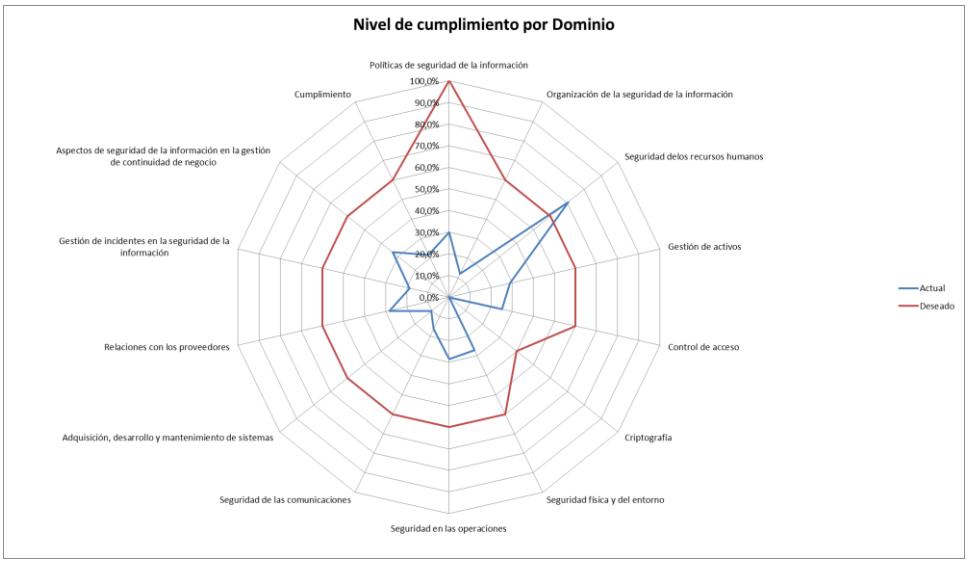

Gráfico No. 9: Nivel de Cumplimiento por Dominio

Considerando los dominios de la seguridad de la información y su nivel de cumplimiento en la gráfica se observa que en relación con las metas planteadas para los 3 próximos años, el dominio Seguridad de los Recursos Humanos creció en un 70%, la Política de Seguridad de la información en un 30%, Aspectos de seguridad de la información en la gestión de continuidad de negocio en un 33%, Gestión de activos, Seguridad en las operaciones y Relaciones con los proveedores en 28% aproximadamente, los demás distan ampliamente de las metas esperadas.

8.4.3. Informe de Auditoría de cumplimiento

El informe de auditoría se presenta en el archivo:

Anexo 13 - IAI-013_INFORME DE AUDITORIA. Pdf.

Según lo encontrado en la auditoría podemos observar que en esta etapa de organización el SGSI, aún no se encuentra muy afianzado, en cuanto que algunos controles no están plenamente implantados.

Sin embargo en este primer proceso de auditoría, se muestra un gran compromiso del personal de la empresa.

A continuación en la tabla No. 17 se resume las no conformidades referentes a los distintos dominios de la ISO 27002:2013, de acuerdo al estado actual de la empresa. Se estudia de cada uno de los controles de los respectivos dominios:

NORMA ISO 27001:2013		NC MAYOR	NC MENOR	OPORNUTIDAD DE MEJORA
5	Políticas de seguridad de la información	0	0	1
6	Organización de la seguridad de la información	0	3	3
7	Seguridad delos recursos humanos	0	0	1
8	Gestión de activos	0	3	3
9	Control de acceso	0	4	4
10	Criptografía	0	0	2
11	Seguridad física y del entorno	0	2	5
12	Seguridad en las operaciones	0	9	2
13	Seguridad de las comunicaciones	0	4	1
14	Adquisición, desarrollo y mantenimiento de sistemas	0	4	3
15	Relaciones con los proveedores	0	1	2
16	Gestión de incidentes en la seguridad de la información	0	2	3
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0	2	0
18	Cumplimiento	0	3	2

Tabla No. 17: Resumen No Conformidades

8.4.3.1. CONCLUSIÓN FINAL

La auditoría encontró que no se está haciendo la revisión de los controles ya establecidos y que es insuficiente la documentación de los procesos. Determinando además que ciertos procedimientos resultan no adecuados para dar cumplimiento a lo exigido por la norma.

8.4.3.2. RECOMENDACIONES

Es necesario que la empresa reajuste su cronograma en cuanto a la finalización de implementación de los controles y la fecha de posible certificación.

También es necesario que la empresa destine los recursos planteados para la ejecución de los proyectos e implantación de los controles en especial aquellos de mayor incumplimiento como son la Seguridad en las operaciones, la seguridad de las comunicaciones y Adquisición, desarrollo y mantenimiento de sistemas. Y otros que podrían afectar directamente la obtención del certificado, como el dominio de Cumplimiento.

9. BIBLIOGRAFÍA Y REFERENCIAS

1. Material no publicado. Documentación oficial de la empresa de Estudio.
2. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC-27001. (2013). TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN– REQUISITOS.
3. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC-27002. TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
4. IT Governance Institute. (2007). Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez. COBIT, 4.1, 211.
5. http://www.iso27000.es/iso27000.html
6. INTERNATIONAL STANDARD ISO/IEC 27007. 2011. Information technology – Security Techniques - Guidelines for information security management systems auditing.
7. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vh6vBm6YGjQ.
8. http://www.corporacionloprado.cl/Docs/SGC%20control%20y%20mejora/Revision%20por%20la%20direccion.pdf
9. http://yumbo.univalle.edu.co/Calidad/archivos/MATRIZ%20DE%20ROL%20Y%20RESPONSABILIDADES%20YUMBO.pdf
10. http://www.empopasto.com.co/site/wp-content/uploads/2013/05/P.-49.2-0003-Auditoria-interna-V21.pdf
11. http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_3__analisis_de_riesgos.html
12. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055190#.VkEL7W6YGT1