UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD INGENIERIA

MANUAL DE SEGURIDAD DE LA INFORMACIÓN PARA UN ORGANISMO DEL ESTADO COLOMBIANO

MANUAL SAFETY INFORMATION TO STATE COLOMBIAN AGENCY

Alumno
Juliana Andrea Santamaría Ramírez
Profesional en Comercio Internacional
u6700587@unimilitar.edu.co

Bogotá, Julio del 2014

MANUAL DE SEGURIDAD DE LA INFORMACIÓN PARA UN ORGANISMO DEL ESTADO COLOMBIANO

MANUAL SAFETY INFORMATION TO STATE COLOMBIAN AGENCY

Juliana Andrea Santamaría Ramírez
Profesional en Comercio Internacional
Universidad Militar Nueva Granada, Bogotá, Colombia
u6700587@unimilitar.edu.co

RESUMEN

El manual de seguridad de la información permite determinar las fortalezas y debilidades que tiene la organización frente a los activos de información, conocer el estado actual ante seguridad de información y sus controles, con el fin de crear estrategias que minimicen las amenazas que impactan la vulnerabilidad organizacional. Basado en una investigación de campo y documental se pudo establecer el nivel de madurez actual en que se encuentra la organización por medio de encuestas, revisión de documentos e igualmente, se realizaron visitas a las instalaciones y se revisaron aspectos de seguridad física haciendo una valoración inicial a los controles establecidos por la Norma ISO 27001:2013. La creación de políticas pertinentes y aplicables, basadas en el análisis y evaluación de riesgo de las informaciones obtenidas de los activos que son permitidas valorar, es el resultado de la investigación realizada a la organización. Para conseguir la efectividad esperada del Sistema de Gestion de seguridad de la información, fue necesario quemar etapas específicas y en un orden determinado, calculado entre 6 y 12 meses, dependiendo del grado de madurez actual de seguridad de la información y el alcance. El hecho de que la organización quiera vivir actualizada y de haber tomado la decisión de transformar desarrollar y estar siempre en un nivel competitivo, hace parte de la estrategia de la organización que quiere la mejora continua, siempre bajo el marco legal y normativo. Con un Sistema de Gestion de Información la organización conoce los riesgos a los que está sometida su información y los asume, los sistematiza, documenta, da a conocer, revisa y mantiene actualizados.

Palabras Claves: Seguridad, Información, Riesgos, Controles, Activos

ABSTRACT

The handbook of information security to determine the strengths and weaknesses that the organization against information assets, to know the current state of information security and controls, in order to create strategies to minimize threats impacting vulnerability organizational. Based on field research and documentary were able to establish the current level of maturity which is the organization through surveys, document review and likewise, site visits were conducted and physical security aspects were reviewed by an initial assessment controls established by ISO 27001:2013. Creating relevant and applicable policies, based on risk analysis and assessment of the information obtained from the assets that are allowed to assess, is the result of research on the organization. To achieve the expected effectiveness of the Management System of Information Security, it was necessary to burn specific stages and in a certain order, estimated at between 6 and 12 months, depending on the current maturity of information security and range. The fact that the organization wants to live updated and I made the decision to transform and develop always be at a competitive level, is part of the strategy of the organization that wants continuous improvement, always under the legal and regulatory framework. With a Management Information System organization knows the risks that your information is submitted and assumes, the systematized, documented, disclosed, reviewed and kept up to date.

Key words: Security, Information, Risk, Controls, Assets

1. INTRODUCCION

La Norma ISO 27001:2013, (1) es sencilla de implementar? **NO**, en este mundo que es cada vez más competitivo y globalizado, en donde a las empresas les corresponde buscar nuevas vías que les permita tener y mejorar sus ventajas, tienen a la mano una herramienta que les permite convertirse en empresas más versátiles mejorando su seguridad protegiendo los activos de mayor valor, implementando controles para la gestión de las amenazas presentes y futuras.

Un sistema de Gestion de seguridad de la Información es un proceso sistemático, documentado y debe ser conocido por toda la organización. (2) Le gustaría garantizar un nivel de protección total pero es imposible. Su propósito es, garantizar que los riesgos de la seguridad sean conocidos, asumidos y minimizados por la

organización de una manera documentada, sistemática, estructurada, y adaptable a los cambios que se produzcan.

Las organizaciones son dependientes actualmente de sus redes informáticas y un problema que les afecte así sea mínimo, puede comprometer las operaciones, que se traducen en pérdidas económicas, retrasos y crisis de confianza por parte de los usuarios.

Las instituciones del Estado acumulan una gran cantidad de información, empleados, clientes, servicios productos redes, informantes, que son fundamentales que son importantes para su organización (3). Esta información está amenazada por la delincuencia informática poniendo en riesgo la base de datos de la organización. La seguridad de la información es una disciplina que tiene como principios básicos proteger la confidencialidad, integridad y disponibilidad de la información.

Implementando estrategias que cubran los procesos para la prioridad de la organización son los activos.

Existe la seguridad de la información tanto desde el punto de vista físico que se refiere a la seguridad de un equipo informático (hardware), (4) y la seguridad lógica que se refiere a la seguridad de la información y los programas almacenados en un equipo una red de datos.

La información confidencial de una institución o entidad es un requisito, por tanto la seguridad debe ser un proceso continuo de mejora, donde las políticas y controles deben estar actualizados revisados periódicamente. (5)

De allí la importancia de analizar y evaluar los riesgos a los cuales estos pueden estar sometidos y así minimizar los efectos.

1.1 CONTEXTO DE LA ORGANIZACION

Este organismo del estado, Es una entidad de inteligencia del gobierno Colombiano que se encarga con todo lo relacionado de la seguridad de la información, con este propósito trabajan diferentes especialistas en busca de información. Sirve de enlace y combina las acciones con las diferentes fuerzas.
Su función es proteger, recopilar y mantener la seguridad de la información.

Ante la evidencia vivida en la Guerra de Corea, donde hombres del Ejército Nacional lucharon junto a los mejores guerreros del mundo, se notó la falencia en el área de Inteligencia. Es por esto que el día 02 de Febrero de 1962 un grupo de Oficiales

Superiores del Ejército Nacional, entre ellos el Señor Teniente Coronel RICARDO CHARRY SOLANO, son seleccionados por el Comando de la Fuerza para realizar un curso de Inteligencia en FORT HALABIRD (EE.UU.).

A su regreso entre el 24 de Octubre de 1962 y el 16 de Enero de 1963, en una de las aulas de la Escuela de Artillería del Ejército, se lleva a cabo el primer Curso de Inteligencia y Contrainteligencia para Oficiales de las Fuerzas Militares. Posteriormente el 15 de Marzo de 1963, se da inicio al primer Curso de Inteligencia para Suboficiales. El Comando del Ejército mediante disposición No. 020 del 02 de Noviembre de 1964 crea el Batallón de Inteligencia y Contrainteligencia BINCI, respondiendo a la necesidad de contar con una Unidad especializada en labores de Inteligencia. En el año 1965, el destacamento de Inteligencia se trasladó a las antiguas instalaciones del Hospital Militar en San Cristóbal, donde inició con gran entusiasmo su labor.

Ante la excelente labor desarrollada por la Inspección de Estudios del Batallón de Inteligencia, el Comando General de las Fuerzas Militares, mediante disposición No. 021 del 29 de septiembre de 1982, le da el carácter de Unidad Especial (Escuela).

Mediante Resolución No. 612 de 1985, son aprobadas las Disposiciones No. 002 del 24 de Enero de 1985 del Comando del Ejército y No. 003 del 01 de Febrero de 1985 del Comando General de las Fuerzas Militares, por medio de las cuales se crea el BATALLÓN ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA BRIGADIER GENERAL RICARDO CHARRY SOLANO, en homenaje a este gran hombre "Artífice de la Inteligencia Operativa del Ejército Nacional".

El día 09 de Abril de 1991, por disposición del Comando Superior, la Escuela de Inteligencia se traslada a las antiguas instalaciones de la Escuela Superior de Guerra, dentro de la Escuela Militar de Cadetes General José María Córdova. El 7 de noviembre de 1997 fue reubicada en el sector Guaymaral. El 20 de diciembre de 2000 la Escuela ocupa un alojamiento de tropa en predios de la Escuela de Infantería, donde funcionó hasta el 30 de Julio de 2002 fecha en que fueron inauguradas sus propias instalaciones. (6)

El 04-MAR-92, mediante oficio No. 3077-, el Comando del Ejército, aprueba el lema del Arma de Inteligencia: CAVE PRO PATRIA, "EN GUARDIA POR LA PATRIA". El lema fue propuesto por la Escuela de Inteligencia.

2. MATERIALES Y MÉTODO

2.1 MATERIALES

A continuación se lista la normatividad asociada a este trabajo:

- **Norma ISO/IEC 27001 2013:** “Tecnología de la Información – Técnicas de Seguridad - Sistemas de gestión de seguridad de la información (1, www.bogotaturismo.gov.co)
- **SO/IEC 27002 2005:** ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES (7)

2.2 MÉTODO

El método utilizado fue el descriptivo – documental, cuya fuente de información fueron las personas vinculadas a los procesos, las leyes, decretos, resoluciones y normas, a través de técnicas de observación sistemática que permitieron cuantificar las variables de interés, permitiendo determinar el estado del sistema de información de la empresa objeto, identificando sus factores más relevantes.

En este trabajo se evalúa la seguridad de la información a la luz de los controles de la ISO 27001:2005. El desarrollo de este se llevó en tres pasos: la primera consistió en una investigación documental, la segunda en una investigación de campo y la tercera es el análisis, evaluación y tratamiento de riesgos de los activos.

El levantamiento de la información a través de encuestas, auto evaluación, y visitas a las instalaciones con el personal adscrito a la organización.

Esta metodología se desarrolla con el Método de SHEFFI (8) para el análisis de riesgo y metodología de (Alexander 2007) para la gestión de evaluación de riesgos y la escala de Likert (9) (método de evaluación primaria) Es una escala psicométrica comúnmente utilizada en cuestionarios y es la escala de uso más amplio en encuestas para la investigación.

2.2.1 Estado del arte del manual de seguridad

El manual de seguridad de la información, inicia su desarrollo e implementación noviembre del año 2013, su construcción y elección fue por etapas; por medio de la primera sesión la organización determina la necesidad de conocer el riesgo de los activos de información y determina la creación del manual de seguridad de la información.

Se crea el organigrama de la organización para este proceso y se conforman el Sistema Administrativo de Seguridad de la Información que tiene como funciones la toma de decisiones, apoyo, implementación y capacitación para la aplicación del manual de seguridad de la información. *Ver Organigrama*

Un SGSI incluye cuatro fases:

- Manual de Seguridad
- Procedimientos
- Instrucciones chequeo de listas, formularios
- Registros

La organización determino la creación del manual de seguridad con todas las áreas de la organización, excepto las de información secreta y vulnerables para el estado.

El primer paso que se realizó fue la evaluación actual de la organización en cuanto a seguridad de los activos por medio de un auto evaluación inicial, encuestas y visitas físicas a las instalaciones y personal operativo; se obtuvo el inventario de los activos de información por clasificar.

Se determinó en la sesión con la Comisión de Seguridad de la información el inicio de la creación e implementación del manual de seguridad luego de hacer esta investigación inicial. Para así conocer en qué nivel de riesgo están los activos de información de la organización y determinar que políticas implementar.

2.2.2 Generación del alcance y la política de seguridad informática

En la implementación de un sistema de gestión de seguridad de la información, el alcance y la política de seguridad son documentos esenciales para determinar los límites de la investigación ya que no tiene por qué abarcar toda la organización si no lo que realmente necesita tratamiento y que tienen influencia sobre la seguridad de la información. La política de seguridad de la información es una declaración de intenciones de parte de la dirección de la organización respecto al manual de seguridad.

El alcance de un manual de seguridad contiene:

- Descripción de la empresa
- Delimitación del Alcance
- Descripción de la organización dentro de la empresa

La política de seguridad de la información tiene por objeto:

- Establecer objetivos con relación a la seguridad de la información.

- Cumplimiento de requisitos legales
- Realizar el análisis de riesgo.

Por esta razón se determinó conjuntamente con la organización para el alcance la ubicación física, disponer de los organigramas organizativos, los requisitos legales y contractuales relacionados con la seguridad de la información.

En cuanto a la política de seguridad se establecieron los objetivos de seguridad, los criterios de evaluación del riesgo y la aprobación de la dirección.

2.2.3 Valoración de los controles basado en la ISO27001:2013

La norma ISO 27001: 20013 establece 133 controles en el Anexo A de la norma, con el objetivo de establecer medidas de seguridad, estos controles sirven para saber cuáles la organización va implementar, y los elegidos como se realizara su implementación y hacer la Declaración de aplicabilidad

Se realizó mediante sesión con el sistema administrativo la evaluación inicial de los controles y determinar cuáles controles se implementan.

2.2.4 Análisis y evaluación de riesgos

En este nivel se definió el enfoque de evaluación de riesgos mediante una metodología de evaluación de riesgos adecuada para el SGSI encontrada en la ISO 27005.

Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar que sean falsos y subjetivos.

Este método determino:

- Los activos con mayor valor para la organización que están dentro del alcance y sus responsables directos.
- Identificar las amenazas relevantes de los activos.
- Identificar las vulnerabilidades.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

2.2.5 Manual de seguridad propuesto

Producto de la investigación se creó el manual de seguridad de la información con el objeto de que sea un instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información, de la superación de las fallas y de las debilidades, para así poder cumplir con el objetivo de proteger la información.

Así se desea cumplir con los estándares de seguridad de los sistemas de seguridad de la información garantizando la confidencialidad de los datos.

El objetivo del manual de seguridad es:

- Disminuir la amenaza a la seguridad de la información.
- Evitar el uso indiscriminado de la información.
- Cuidar y proteger los recursos de la organización.
- Concientizar a la organización en general sobre la importancia del uso seguro de la información.

Desde el mes de noviembre del año 2013 se realiza el manual de seguridad cumpliendo las seis etapas hasta el mes de junio del año 2014. Con resultados positivos.

Se implementó:

- El alcance y Política de seguridad.
- Se determinó la metodología de evaluación de riesgos y análisis
- Informe de evaluación de riesgos
- Plan de tratamientos de riesgos
- Declaración de aplicabilidad.

3. RESULTADOS Y ANÁLISIS

A partir del diagnóstico realizado se presentan los resultados obtenidos

3.1 ESTADO DEL ARTE

Para que **La organización del estado que presta un servicio de Protección y cuidado a la Soberanía Nacional Colombiana,** lograra la implantación y diseño del **Manual De Seguridad** se realizaron las siguientes actividades.

1. **Actividad:** Elaboración del Organigrama.
   Para lograr esta actividad la organización debe:

Crear el Sistema de Administrativo de Información que está conformado de la siguiente forma:

Organigrama

Figura 1. Organigrama para el Sistema de Gestión de seguridad de la información
Fuente Propia

- **Comisión de Seguridad de la Información**

La comisión de Seguridad de la Información, son los asesores de la Organización en temas relacionados con la seguridad de la información dentro de la organización que afecta a nivel nacional. Con el fin de generar credibilidad y confianza protegiendo la información de las entidades adscritas a esta Organización.

La Comisión de Seguridad de la Información estará compuesta por los siguientes miembros que tendrán voz y voto:

- El Comandante, quien la presidirá.
- El Ejecutivo, quien ejercerá la coordinación general y oficiara como articulador del SGSI.
- El Ejecutivo, como representante de la Organización Y responsable de la Seguridad Nacional.

Funciones de la Comisión de Seguridad de la Información

La Comisión de la Seguridad de la información es el escenario ideal para que los responsables creen los planes y estrategias de acción para garantizar adecuadamente la seguridad de la información. Permitirá la aprobación de políticas,

acciones y controles a ser implementados por la entidad para fortalecer su estado en seguridad de la información para así proteger adecuadamente la información de los ciudadanos.

- **Grupo Técnico de Apoyo**

La Comisión , es asesorada por el Grupo Técnico de Apoyo, cuya función principal es acotar, dentro de los parámetros establecidos en las normas pertinentes, a nivel táctico y técnico especificando las políticas, objetivos de control y controles propuestos para que sean implementados por cada una de las entidades objetivo.

Es el encargado de la preparación de los documentos, políticos, lineamientos estandar4es y recomendaciones que son avalados por la comisión. Proporciona apoyo técnico y jurídico.

Funciones del Grupo de Técnico de Apoyo

Dentro de las funciones del Grupo Técnico de Apoyo se encuentran:

- Plantear las políticas, controles y lineamientos que componen el Sistema.
- Coordinar los acuerdos de cooperación en temas técnicos y jurídicos.
- Asesorar la comisión.
- Proponer mejoras al Sistema

- **Equipo de gestión al interior de la Entidad**

El equipo de gestión al interior de la entidad se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el SGSI, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

Equipo:

- Líder de proyecto
- Oficial de seguridad de la información
- Personal de seguridad de la información
- Un representante del área de tecnología
- Un representante de sistema de gestión de calidad.

2. **Actividad:** Evaluación del Estado inicial
   Para cumplir con esta actividad la organización debe:

La organización creo los formatos para la evaluación.

- **Evaluación**

Diligencie el siguiente formulario para determinar el nivel de seguridad de la información.

Tabla 1- formato para la entidad

Requisitos	**Cumple SI /NO**	
La entidad cuenta con un líder.	x	
La entidad cuenta con el comité de seguridad.		x
La entidad cuenta con el oficial de seguridad.		x
La entidad cuenta con personal técnico para la seguridad de la información.		x
La entidad cuenta con la integración con otros sistemas de gestión.	x	
La entidad cuenta con apoyo y participación de control interno.	x	
Los funcionarios conocen sus responsabilidades respecto a la seguridad de la información.		x
Los proveedores conocen sus responsabilidades respecto a la seguridad de la información		x

Fuente: el autor

- **Auto evaluación del nivel de gestión de seguridad de la información**

Diligenciar el siguiente formato.

Tabla -2 Formato determinar el nivel seguridad de la organización

Nivel	**Requisitos**	**Cumple**	
		si	no
Plan de seguridad nivel inicial	La entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta. Para ello, deberá implementar las siguientes acciones:		
	a) Identificar el nivel de conocimiento al interior, en temas de seguridad de la		X

	información y seguridad informática. b) Definir la política de seguridad a ser implementada. c) Divulgar la política de seguridad al interior de la misma. d) Conformar un comité de seguridad o asignar las funciones de seguridad al comité. e) Identificar los activos de información en los procesos incluyendo los activos documentales (records), de acuerdo con el análisis de procesos realizado. f) Identificar los riesgos y su evaluación, en dichos procesos. g) Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados	x	X X X X x
Plan de Seguridad Nivel básico	Con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles	X	
	De acuerdo con el plan de capacitación definido por la entidad en el nivel inicial, esta ejecuta las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan	x	

3. **Actividad:** Inventario de los Activos
   Para cumplir esta actividad la organización debe:

La organización hace el inventario de activos, por medio de documentos escritos e impresos con la categoría de ***información clasificada***, también realiza visitas a la instalaciones físicas.

Se presenta una imagen de una parte del inventario de activos.

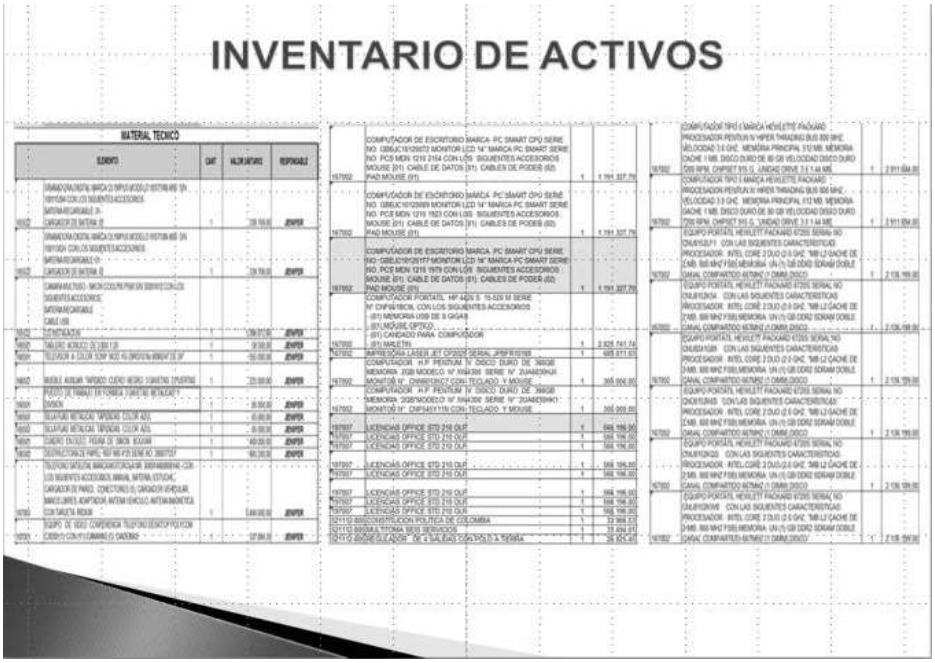

Figura 1: Inventario de Activos
Fuente: Propia

3.2 GENERACIÓN DEL ALCANCE Y LA POLITICA DE SEGURIDAD

3.2.1 El alcance queda sometido al SGSI, se incluyó una identificación clara de las dependencias, relaciones y límites entre el alcance y aquellas partes que no hayan sido consideradas.

El Sistema de Gestión documentado en este Manual de seguridad de la información aplica a las decisiones y actividades desarrolladas por **La organización del estado que presta un servicio de Protección y cuidado a la Soberanía Nacional Colombiana**, y, aplica a las dependencias que hacen parte dela organización, a procesos internos y externos, a terceros y al personal de la organización; relativas a:

1. Identificación de activos de información y físicos de importancia para la organización.

2. concientizar al personal de la importancia de la seguridad de la información.

A todos los niveles de la organización, en sus instalaciones.

_____ _____

Comandante Ejecutivo

Marzo 2014 Rev.: 0

3.2.2 La política de seguridad de la información es el conductor con el SGSI, ajusta las políticas del Sistema Administrativo, y los requisitos respecto a la seguridad de la información. La política de seguridad de la información es la declaración general que representa la posición de la administración de esta organización del estado con respecto a la protección de los activos de información (los funcionarios, los procesos, la tecnología que incluye hardware y software, la información) a la implementación del SGSI y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

El Organismo del estado que presta un servicio de protección y cuidado a la Soberanía Nacional Colombiana, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores, establece la función de seguridad de la información en la Organización, con el objeto de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de las funciones administrativas.
- Mantener la confianza dentro de la organización.
- Apoyar la innovación tecnológica.
- Implementar el Sistema de Gestión de Seguridad de la información
- Proteger los activos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Identificar violaciones de la seguridad de la información necesarias a todas las partes interesadas que tengas acceso a estas.

Todo usuario es responsable por proteger la información del Organismo del estado que presta un servicio de protección y cuidado a la Soberanía Nacional Colombiana, y dar a conocer cualquier situación que represente desvío o violación de seguridad de esta, así como de atender las recomendaciones pertinentes, presentes en este Sistema de gestión de Seguridad de la información y el Código de Ética.

_____ _____

Comandante Ejecutivo

Marzo 2014 Rev.: 0

3.3 VALORACIÓN DE LOS CONTROLES BASADO EN LA ISO27001:2013

3.3.1 Auto evaluación de políticas, controles, métricas

Diligencia el siguiente formato para determinar el progreso en la implementación de controles

Tabla -3 Controles de anexo A del estándar ISO 27001 y dominios a los que pertenece.

N°	Dominio - Control		#Ctrls	Cumplimiento
A5	**Política de seguridad de la información** Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.		2	
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.	1	Inexistente
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.	1	Inexistente
A6	**Organización de la seguridad de la información** Gestionar la organización de la seguridad de información.		11	
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.	1	Inicial
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.	1	Inicial
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.	1	Inexistente
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).	1	Inexistente
A.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.	1	Repetible
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.	1	Inicial
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.	1	Inexistente
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.	1	Inicial
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.	1	Inexistente
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.	1	Inexistente
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad , que abarcan los requerimientos de SI relevantes.	1	Inicial
A7	**Gestión de activos de información (AI)** Lograr y mantener la protección apropiada de los activos de información		5	
A.7.1.1	Responsabilidad por los activos	Se mantiene un inventario de AI.	1	Repetible
A.7.1.2		Todo AI tiene asignado un responsable (propietario).	1	Repetible
A.7.1.3		Se dispone de una normativa de uso de los AI	1	Inicial
A.7.2.1	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad	1	Inexistente
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.	1	Inexistente
A8	**Seguridad de los recursos humanos** Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información.		9	
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidadesde de SI, de todo el personal.	1	Inexistente
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.	1	Definido
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.	1	Repetible
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.	1	Inicial
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.	1	Inexistente
A.8.2.3		Se tiene establecido un procesos disciplinario ante el incumplimiento de SI.	1	Repetible
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.	1	Inexistente
A.8.3.2		Se procura la entrega de activos al término de contrato.	1	Inexistente
A.8.3.3		Se retira los derechos de acceso al término del contrato.	1	Inicial

Fuente: Norma ISO 27001 ANEXO

Figura 4. Escala para ANEXO A ISO 27001

Tabla de Escala para ISO27001 e ISO27002		
Calificación		**Descripción**
N/A	No Aplica	No aplica.
0	Inexistente	**Total falta de cualquier proceso reconocible**. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
20	Inicial	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. **No hay procesos estandarizados**. La implementación de un control depende de cada individuo y es principalmente **reactiva.**
40	Repetible	**Los procesos y los controles siguen un patrón regular.** Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. **No hay formación ni comunicación formal** sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
60	Definido	**Los procesos y los controles se documentan y se comunican**. Es poco probable la detección de desviaciones.
80	Gestionado	Los controles se monitorean y se miden. Es posible **monitorear y medir el cumplimiento de los procedimientos** y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
100	Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de **mejores prácticas**, basándose en los resultados de una **mejora continua.**

Fuente: El autor, http://www.revistaespacios.com/a10v31n01/10310152.html

3.4. ANALISIS DEL CUMPLIMIENTO DE LA NORMA ISO 27001:2013

Desde el año 1999 la organización tiene establecido un único procedimiento para la protección de la información, no tiene nada estandarizado, ni dada formalmente establecido, los controles son mínimos. Y son muy pocos los controles que cumple la organización frente al Anexo A de la norma. Siendo su mayor falencia porque afecta el 99% de la organización.

Su forma de custodiar la información es mediante la tabla de retención. La parte esencial de la norma ISO 27001:2013 es la relación con la gestión del riesgo, en esta norma en el Anexo A propone los controles, que debe seleccionar la organización, luego de su evaluación y análisis, se encontraron bastantes incumplimientos, dentro de los más importantes están:

- No hay compromiso dela alta dirección
- No está determinado el alcance.
- No tiene establecido política de calidad.
- No existe metodología de Análisis de Riesgos, identificación de riesgos, Análisis y evaluación de riesgos.
- No existen selección de objetivos de control ni controles.
- No existe conciencia de la importancia de la seguridad de los activos de información.
- No consta plan de auditorías, ni nunca se ha hecho una.

En la tabla 1. Se muestra el grado de cumplimiento a la norma de la organización en el momento de evaluación inicial

Tabla. 1 Calificación de Riesgos

Numeral	Requisito ISO/IEC 27001	Cumplimiento	Observaciones
4	**Sistema de gestión de seguridad de la información**	**32%**	
4.1	Requerimientos Generales	0%	No existe una política definida para el SGSI en la empresa.
4.2	Requerimientos generales	6%	La empresa no ha implementado un plan para el tratamiento de riesgos relacionados con seguridad de la información ni ejerce un adecuado control sobre ella para lograr los objetivos.
4.2.1	Establecer el SGSI	0%	
4.2.2	Implementar y operar el SGSI	0%	
4.2.3	Monitorear y revisar el SGSI	0%	
4.2.4	Mantener mejorar el SGSI	0%	
4.3	Requerimientos de documentación	10%	No existe control de documentos ni registros solo un archivo sin procedimientos.
4.3.1	General	0%	
4.3.2	Control de documentos	8%	
4.3.3	Control de registros	8%	
5	**Responsabilidad de la gerencia**	**27%**	
5.1	Compromiso de la gerencia	2%	No existe una política no existe ningún presupuesto pan plan de SGSI
5.2	Gestión de recursos	20%	
5.2.1	Provisión de recursos	5%	
5.2.2	Capacitación, conocimiento y capacidad	0%	
6	**Auditorías internas SGSI**	**0,0%**	No se cuenta con un programa de auditoría interna para el SGSI.
32307	**Revisión Gerencial del SGSI**	**0,00%**	
7.1	General	0%	No existe
7.2	Insumo de la revisión	0%	
7.3	Resultado de la revisión	0%	
8	**Mejoramiento del SGSI**	**30%**	
8.1	Mejoramiento continuo	10%	No existe plan de auditorías nunca se ha hecho
8.2	Acción correctiva	10%	
8.3	Acción preventiva	10%	
Cumplimiento de la Norma		**4.45%**	

Fuente: Se toma idea de la tabla 4. Calificación de Riesgos del artículo MAPA DE RIESGO PARA EL SISTEMA DE MANEJO DE LA INFORMACIÓN EN UNA EMPRESA DEL SECTOR SALUD Janeth Patricia Rodríguez Chabur

La organización cumple con un 4.45% del cumplimiento de la norma, lo cual demuestra un nivel muy bajo respecto a la seguridad de la información.

3.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Este estudio se plantea para la evaluación de los activos de información a la luz de los controles de la norma ISO 27001:2013

Es una investigación de campo porque se inicia haciendo un análisis de los problemas sistemáticos entendiendo su naturaleza y posibles causas y sobre todo efectos.

La población estuvo conformada por el total del personal de la organización.

Se llevó a cabo la recolección de la información, por medio de encuestas y visitas guiadas.

3.5.1 Estructura del documento

Las secciones siguientes presentan:

- La primera sección describe la clasificación de los activos.
- La segunda sección Se realiza la tasación de activos.
- La tercera sección describe la metodología de análisis y evaluación de riesgos, la identificación de vulnerabilidad. Se calcula la amenaza y vulnerabilidad.
- La cuarta sección tiene análisis de riesgos.
- La quinta sección es evaluación del riesgo.

Para realizar el análisis de riesgos de dichas variables se definieron cada una de las tablas para realizar la evaluación.

3.5.2 Clasificación de los activos

En ese mismo orden de ideas, debe existir una adecuada gestión de los activos para poder mantener una adecuada protección de los mismos en la empresa (Peltier, 2001). ((9))

Las categorías a utilizar en esta metodología para clasificar los activos se basan en ISO 17799:2005:

Tabla 2. Categorías de Clasificación de Activos

• Activos de información (datos, manuales de usuario, entre otros)
• Documentos en papel (contratos)
• Activos de software (aplicación, software de sistemas, entre otros)
• Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)
• Personal (estudiantes, clientes, empleados, entre otros)
• Imagen de la compañía y reputación − Servicios (comunicaciones, entre otros).

Fuente: Propia

Como el inventario es muy extenso se escoge un grupo relevante y manejable de activos, siendo los que tengan más valor. El Criterio de evaluación es personal.

3.5.3 Identificación y tasación de activos

La tasación es la asignación de un valor que para la organización tiene el activo si llegara a dañarse, perderse o divulgarse, es decir, es la asignación en términos de la importancia, en cuanto a su confidencialidad, integridad y disponibilidad.
Para la tasación de los activos se puede utilizar la escala de Likert;

Tabla N 3 Tasación de Activos

NOMBRE DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITERIO
IMPRESORA LASER JET CP2025 SERIAL JPBFR10188	1	4	1	**1= MUY POCO**
COMPUTADOR H.P PENTIUM IV DISCO DURO DE 300GB MEMORIA 2GB MODELO N° XW4300 SERIE N° 2UA6030HJX MONITOR N° CNN6012KC7 CON TECLADO Y MOUSE	3	2	4	**2=POCO**
COMPUTADOR H.P PENTIUM IV DISCO DURO DE 300GB MEMORIA 2GB MODELO N° XW4300 SERIE N° 2UA6030HK1 MONITOR N° CNP545Y11N CON TECLADO Y MOUSE	4	3	3	**3=MEDIO**
LICENCIAS OFFICE STD 210 OLP	2	5	5	**4= ALTO**
LICENCIAS OFFICE STD 210 OLP	2	1	2	**5= MUY ALTO**

Fuente: Propia

3.5.4 Descripción de Método de Amenazas y Vulnerabilidades

Los activos de información están expuestos a múltiples formas de amenazas. Una amenaza puede causar un incidente no deseado que genera daño a la organización

y sus activos (Alexander, 2007), o existencia de algún mecanismo, que activado, permite explotar una vulnerabilidad.

- **Las amenazas se pueden clasificar en**:

- **Naturales** (inundaciones, terremotos, maremoto, incendios, entre otros)
- **A instalaciones** (caída de energía, explosión, fallas mecánicas, entre otros)
- **Humanas** (huelgas, pérdida de clave personal, epidemias, entre otros)
- **Tecnológicas** (virus, hacking, pérdida de datos, fallas en la red, fallas, entre otros)
- **Operacionales** (crisis financieras, fallas en equipos, entre otros)
- **Sociales** (sabotaje, motines, bombas, protestas, entre otros)

Para cada activo, se deben identificar las distintas amenazas que lo pudieran afectar, y se debe medir la posibilidad de su ocurrencia. Se recomienda usar la escala de Likert, (9) donde:

Tabla 4 Escala de Likert

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

Fuente Propia

Una vulnerabilidad es una debilidad de seguridad asociada a los activos de información, en otras palabras, es una condición que permite que una amenaza afecte un activo. Por lo que, una vulnerabilidad es un estado que le permite a una amenaza producir un daño sobre la organización.

- **Las vulnerabilidades se pueden clasificar en**:

- **Seguridad de los recursos humanos** (falta de mecanismos de monitoreo, falta de políticas para el uso de las telecomunicaciones, carencia de conciencia en seguridad, falta de entrenamiento en seguridad, entre otros)
- **Control de acceso** (falta de políticas se seguridad respecto a las pantallas, falta de protección de los equipos, passwords sin modificaciones frecuentes, falta de políticas de control de acceso, entre otros)
- **Seguridad física y ambiental** (control de acceso físico inadecuado a oficinas y edificios, condiciones físicas no adecuadas, falta de equipos de protección de variación de voltaje, entre otros)

- **Gestión de operaciones y comunicaciones** (interfaces de usuarios complicada, inadecuado control de cambio, inadecuada gestión de red, entre otros)
- **Mantenimiento, desarrollo y adquisición de sistemas de información** (falta de protección de llaves criptográficas, carencia de políticas para el uso de criptografías, falta o carencia de políticas de validación de datos, entre otros).

Para que una amenaza pueda causar daño a un activo de información, tendría que explotar alguna vulnerabilidad del sistema, aplicación o servicio usados por la organización.

Una vez que se identifiquen las vulnerabilidades, para cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza. En este punto se puede hacer uso de la escala de Likert.

Tabla 5 Escala de Likert

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

Fuente Propia

3.5.5 Calcular Amenazas y Vulnerabilidades

Una vez que se han identificado las amenazas y vulnerabilidades, se procederá a calcular la probabilidad que se pueda presentar conjuntamente y causar un riesgo. El riesgo es la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Peltier, 2001). Se recomienda hacer uso de la escala de Likert. El campo Total se obtiene de la multiplicación de la probabilidad de la amenaza y su correspondiente vulnerabilidad.

Tabla 6 Calculo de Probabilidad de Amenaza

Activo	Amenaza por naturaleza	Probabilidad ocurrencia	vulnerabilidad	total	priorización
Computador portátil	2	3	2	9	3
Licencia	2	3	3	9	3

Fuente propia

3.5.6 Análisis de Riesgos

Con el análisis del riesgo se pretende identificar y calcular los riesgos basados en la identificación de los activos, en el cálculo de las amenazas y sus vulnerabilidades.
Existen diferentes maneras de relacionar los valores asignados a los activos y aquellos asignados a las vulnerabilidades y amenazas para así obtener mediciones de riesgo (8).

El método aquí recomendado provee un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.
Este método relaciona los factores del impacto económico de la amenaza o importancia para la empresa, dirección, área o departamento, y la probabilidad de ocurrencia de la amenaza, utilizando la escala de Likert.

Tabla 7 Método para cálculo de Riesgo

Activo	**Amenaza**	**Impacto de la Amenaza**	**Posibilidad de la Ocurrencia**	**Medición del Riesgo**	**Priorización**
A		5	3	15	2
B		4	5	20	1
C		1	2	8	4

Fuente Propia

3.5.7 Evaluar riesgos

Una vez que se ha realizado el cálculo del riesgo de todos los activos pertenecientes a la organización, área, dirección o departamento (de acuerdo al alcance definido), se procederá a determinar cuáles son las amenazas cuyos riesgos son los más significativos. Por lo que se deberá preparar una escala que permita medir los niveles de riesgo. Se propone usar los siguientes criterios (Alexander, 2007):

- Impacto económico
- Tiempo de recuperación de la organización, área, departamento o dirección
- Posibilidad de ocurrencia del riesgo
- Posibilidad de interrumpir las actividades

Tabla 8 Escala de Riesgo para valorar su importancia

Riesgo		Criterios para Evaluar la importancia del Riesgo				
Activos	Amenazas	Impacto Económico	Tiempo recuperación	Probabilidad de Ocurrencia	Probabilidad de interrumpir actividad	Total
A	AAA	5	3	3	1	3

Fuente Propia

Con estos criterios se prepara unos datos, tal como se muestra en la Tabla 4, utilizando la escala de Likert, con la finalidad determinar los grados de importancia que representan las amenazas para la empresa. El campo Total se obtiene de la suma de los campos criterios para evaluar la importancia de riesgo, dividido entre 4.
Una vez identificado los niveles de riesgo para aquellos activos cuyos niveles y estimación de daño se consideren altos, se requiere que la organización tome acción, y por ende, deben estar sujetos al tratamiento de inseguridad y al proceso de toma de decisión de la gerencia.

Se seleccionan los riesgos con mayor puntuación, para una acción de tratamiento de riesgo inmediato para su eliminación.

3.6 MANUAL DE SEGURIDAD DE LA INFORMACIÓN PROPUESTO

Los documentos que conforman el manual de seguridad son:

- Alcance, Políticas y objetivos de Seguridad.
- Metodología de Evaluación de Riesgos.
- Informe de Evaluación de Riesgos.
- Plan de tratamientos de Riesgos
- Declaración de aplicabilidad

Para esta sección se evidencia con la tabla de contenido del manual de Seguridad.

3.6.1 MANUAL DE SEGURIDAD DE LA INFORMACION

Se presenta una parte de las políticas aprobadas para la declaración de aplicabilidad

3.7. Políticas de Seguridad según Declaración de aplicabilidad

Con el fin de mantener una relación entre el conjunto de políticas se presenta a continuación las políticas de seguridad que soportan el SGSI determinadas por la organización para su funcionamiento.

Política	
Gestión de la operación del servicio por terceras partes. **Objetivo**: Implementar y mantener un grado adecuado de seguridad de la información de conformidad de los acuerdos de prestación del servicio por terceras partes.	
Monitoreo y revisión por los servicios de terceras partes.	**Control**: Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas exigentes de seguridad de la información, en los procedimientos y controles se deben gestionar según la importancia del sistema.
Planificación y aceptación del sistema	
Objetivo: minimizar el riesgo de fallas de los sistemas	
Gestión de la capacidad	**Control**: Se debe hacer seguimiento y adaptación del uso de los recursos.

4 CONCLUSIONES

Entre las principales conclusiones que se obtienen en esta investigación, se encuentra:

- Se evidencia que el personal de la organización no tiene conocimiento básico para la implementación de la organización

- La alta dirección de la organización, establece la importancia de aplicar los controles determinados en la organización y el cumplimiento de las políticas establecidas.
- Se compromete a la concientización y capacitación del personal de las áreas que se aplica el manual de seguridad.
- El conocer el inventario de activos es fundamental para la organización para saber en qué grado están expuestos ante el riesgo.
- La organización decide mantener actualizado el manual de seguridad cumpliendo los requisitos legales
- El desarrollo de este trabajo permite identificar que la implementación y pasos de elaboración del manual de seguridad se ha convierte en una de las prioridades de mayor importancia.
- Que siempre se debe estar buscando la mejora continua

Bibliografía

1. (s.f.). Recuperado el 03 de 07 de 2014, de http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

1. (s.f.). *www.bogotaturismo.gov.co*. Recuperado el 30 de JUNIO de 2014, de http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

2. (s.f.). Recuperado el 04 de 07 de 2014, de http://www.iso27000.es/sgsi.html

3. (s.f.). Recuperado el 2 de 7 de 2014, de www.telecom.go.cr/index.php/publicaciones/.../estado.../download

3. (2007). Diseño de un Sistema de Gestion de Seguridad de la Información. En a. Alexander. bogota: Alfaomega Colombia.

4. (s.f.). Recuperado el 04 de 07 de 2014, de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

5. (s.f.). Recuperado el 3 de Julio de 2014, de https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

6. (s.f.). Recuperado el 14 de junio de 2014, de http://www.esici.edu.co/?idcategoria=217146

7. (s.f.). *www.iso27000.es*. Recuperado el 30 de JULIO de 2014, de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

8. (s.f.). *wikipedia.org*. Recuperado el 30 de junio de 2014, de http://en.wikipedia.org/wiki/Yossi_Sheffi

9. (s.f.). *wikipedia.org*. Recuperado el 1 de julio de 2014, de http://es.wikipedia.org/wiki/Escala_Likert