IMPLEMENTACIÓN DE UN PROCESO DE OPTIMIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA ISO/IEC 27001:2013 PARA EL ÁREA ADMINISTRATIVA DE VENTOLINI S.A. EN EL 2016

YONANTAN DELGADO TAPIA – ID 108411

FRANCISCO ANTONIO RIASCOS SANCHEZ – ID 108735

FUNDACIÓN UNIVERSITARIA CATÓLICA - LUMEN GENTIUM

UNIDAD DE POSGRADOS Y EDUCACIÓN CONTINUA

CALI, VALLE DEL CAUCA

2016

IMPLEMENTACIÓN DE UN PROCESO DE OPTIMIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA ISO/IEC 27001:2013 PARA EL ÁREA ADMINISTRATIVA DE VENTOLINI S.A. EN EL 2016

YONANTAN DELGADO TAPIA – ID 108411

FRANCISCO ANTONIO RIASCOS SANCHEZ – ID 108735

Trabajo presentado como requisito parcial de grado para optar al título de ingeniero de sistemas

HECTOR FABIO OSPINA

FUNDACIÓN UNIVERSITARIA CATÓLICA- LUMEN GENTIUM

UNIDAD DE POSGRADOS Y EDUCACIÓN CONTINUA

CALI, VALLE DEL CAUCA

2016

Dedicatoria

Dedicamos este trabajo a nuestros padres y hermanos que han sido apoyo, luz, consejo y fuerza en cada nuevo proyecto en nuestras vidas.

AGRADECIMIENTOS

Agradecemos a nuestros Padres que con dedicación y apoyo incondicional han estado presentes en cada etapa de nuestras vidas, a nuestros hermanos por fastidiarnos tanto pero sobre todo por estar siempre allí, a nuestras familiares y amigos con quienes compartimos tanto en esta gran etapa, a los ángeles que aparecieron en nuestras vidas en el momento más oportuno para llevarnos en sus alas y sobre todo a Dios que nos dio la vida y los dones necesarios para crecer.

Agradecemos enormemente a la empresa FABRICA DE ALIMENTOS PROCESADOS VENTOLINI S.A. que nos abrió las puertas para el desarrollo de esta actividad, a sus empleados que nos recibieron como parte fundamental del equipo de trabajo y nos ayudaron en todo.

CONTENIDO

AGRADECIMIENTOS v
INTRODUCCIÓN 2
1. PLANTEAMIENTO DEL PROBLEMA 3
2. OBJETIVO GENERAL 4
Optimizar la seguridad de la información en Ventolini S.A. 4
2.1 OBJETIVOS ESPECIFICOS 4
3. MARCO TEORICO 4
3.1 Norma ISO 4
3.3 Magerit V.3 Metodología de Análisis y Gestión de Riesgos 7
3.4 Modelo de Procesos PHVA 9
4 METODOLOGÍA 9
4.1 Metodología aplicada 10
4.2 Antecedentes 11
5 ESTADO DEL ARTE 12
CONCLUSIÓN 13
REFERENCIAS 15
ANEXOS 18

IMPLEMENTACIÓN DE UN PROCESO DE OPTIMIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA ISO/IEC 27001:2013 PARA EL ÁREA ADMINISTRATIVA DE VENTOLINI S.A. EN EL AÑO 2016

IMPLEMENTACIÓN DE UN PROCESO DE OPTIMIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA ISO/IEC 27001:2013 PARA EL ÁREA ADMINISTRATIVA DE VENTOLINI S.A. EN EL 2016

Yonatan Delgado Tapia

yonatandtapia@live.com

Francisco A Riascos Sanchez

Francisco.riascoss@gmail.com

Resumen

Este articulo expone la implementación de un proceso de optimización de seguridad de la información con base en la ISO/IEC 27001:2013 para el área administrativa de VENTOLINI S.A. en el 2016, por lo cual se implementó la metodología PHVA para garantizar el optimo funcionamiento del proceso e inicio con una auditoria para determinar el estado actual de los objetivos de control de la norma, obteniendo un cronograma de acciones correctivas y finalizando con la implementación de mejoras de seguridad de la información.

Palabras claves: *iso/iec 27001:2013, seguridad de la información, phva, auditoria*

Abstract

This article exposes the implementation of a process of safety optimization of the information with base in the ISO/IEC 27001:2013 for VENTOLINI's administrative area S.A. in 2016, departing from an audit to determine the current condition of the aims of control of the norm, generating chronogram of corrective actions and finishing with the implementation of safety improvements of the information. The previous thing implementing the methodology PDCA in the development of the project to guarantee the ideal functioning of the process of safety optimization.

keywords: *iso/iec 27001:2013, information security, pdca, audit.*

INTRODUCCIÓN

A Medida del paso de los años y con la evolución informática que sufren todas las empresas, se vuelve evidente la importancia de la información y su seguridad, además se reconoce que del aseguramiento de los recursos físicos depende la disponibilidad de la información, es por eso que se busca un nivel aceptable de seguridad partiendo del método investigativo para ilustrar el estado del arte en la implementación de un proceso de optimización de seguridad de la información con base en la ISO/IEC 27001:2013 para el área administrativa de Ventolini S.A. en el año 2016 y delinear los procesos bajo la metodología de trabajo PHVA.

Con referencia a lo anterior, se considera necesario la implementación de un proceso de optimización de la seguridad de la información en la empresa Ventolini S.A. mediante el uso de la norma ISO/IEC 27001:2013 de sistemas de gestión de la seguridad de la información, con lo que se proyecta garantizar la implementación del proceso de seguridad de la información.

Es importante resaltar el avance de las leyes colombianas en los últimos años, en ejemplo la ley de protección de datos personales (Alcaldía de Bogotá, 2012), la cual exige el aseguramiento de la información personal por parte de las empresas públicas y privadas del país, generando la implementación de políticas y protocolos de seguridad para garantizar la integridad, disponibilidad y confiabilidad de la información (Isotools, 2015).

De lo anterior y “de acuerdo con el estudio que realizó Fortinet, los ataques cibernéticos dirigidos a entidades gubernamentales tienen impacto en toda la población ya que pueden inhabilitar servicios como suministro de agua potable, electricidad, cámaras de vigilancia, información personal sobre los ciudadanos, transporte aéreo y terrestre, además de las operaciones del Gobierno” (Semana, 2015), puesto que cada día los avances tecnológicos convierten al hombre en un ser dependiente y exigente en una sociedad carente de seguridad.

Las normas de la seguridad surgen como una manera de controlar las fugas o los puntos vulnerables de una organización esto con el fin de mitigar cualquier tipo de violación de la información. Una organización debe contener políticas y procesos que indiquen porque se debe proteger la información u recurso y como va

a ser la manera de brindar la seguridad necesaria para lograr este cometido.

(a) ISO/IEC 27001: Es el estándar más conocido de la familia proporcionando requisitos para un sistema de gestión de seguridad de la información. (ICONTEC, 2015a).

Es adecuada para cualquier organización plantea una mirada completa a la seguridad de la información. Los activos que necesitan protección van de la información digital, documentos en papel y activos físicos (computadoras y redes) a conocimientos de los empleados (ISO/IEC, 2013).

(a) Seguridad de la Información: La información es un activo más de la organización el cual obtiene un valor nominal, por lo tanto, se debe tratar de una manera estructurada, teniendo en cuenta el estado del arte, el avance tecnológico y estructural conlleva que la información sea vulnerable y esté al alcance de toda persona. Observando la seguridad física y del entorno de Ventolini (ISOTools, 2014).

(b) Auditoria: proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría (2002. NTC-ISO 19011. Directrices para la auditoria de los sistemas de gestión de la calidad Y/O ambiental.

1. PLANTEAMIENTO DEL PROBLEMA

Partiendo del hecho que la seguridad de la información “es esencial para mantener la competitividad, los recursos generales, la rentabilidad, el cumplimiento legal y la imagen comercial” (Calder, 2006, p.4). Se puede inferir que la seguridad informática es la mayor fuente de estabilidad para una compañía, pues la mayor parte de la información relevante se encuentra alojada en equipos de trabajo o servidores con diferentes dimensiones y el restante es el conocimiento impartido por cada empleado en sus áreas.

Por ello, para llevar el trabajo a la realidad, nos situamos en la Fábrica de Alimentos procesados Ventolini S.A. encontrando todo un sistema de información sin las bases primordiales para garantizar su seguridad,

todo debido a la falta de políticas de seguridad y el establecimiento de sus respectivos controles.

Todos los Factores anteriores llevan a Ventolini S.A. a ser la mejor empresa para realizar una intervención oportuna y realizar la implementación de un proceso de optimización de seguridad de la información con base en la ISO/IEC 27001:2013 para el área administrativa, mejorando así la seguridad de su sistema de información.

¿Cómo implementar un proceso de optimización de seguridad de la información con base en la ISO/IEC 27001:2013?

2. OBJETIVO GENERAL

Optimizar la seguridad de la información en Ventolini S.A.

2.1 OBJETIVOS ESPECIFICOS

a. Definir por medio de la auditoria el estado actual de seguridad de la información con base a los objetivos de control de la norma ISO/IEC 27001:2013 en el área administrativa de Ventolini S.A.

b. Establecer el procedimiento de implementación de mejora de seguridad de *la información en Ventolini S.A.*

3. MARCO TEORICO

Debido al avance de la tecnología y de la sociedad, que imponen un entorno al alcance de todos con mayores niveles de simplicidad para obtener la información, las organizaciones se enfrentan a la necesidad de implementar los procesos seguridad Informática.

Las normas de la seguridad, surgen como una manera de controlar las fugas o los puntos vulnerables de una organización, esto con el fin de mitigar cualquier tipo de violación de la información. Una organización debe contener políticas y procesos que indiquen porque se debe proteger la información u recurso y como va a ser la manera de brindar la seguridad necesaria para lograr este cometido.

3.1 Norma ISO

ISO (*International Organization for Standardization*, 'Organización Internacional de Estandarización' +, IEC *International Electrotechnical Commission*, ‘Comisión Electrotécnica Internacional’, para el

desarrollo de este trabajo se enfocará en la ISO 27001, 27002, 27005).

ISO 27000 Familia de normas que ayuda a las organizaciones a mantener los activos de información de una manera segura.

El uso de esta familia de normas ayudará a la organización a administrar la seguridad de los activos, como la información financiera, la propiedad intelectual, detalles de los empleados o la información confiada por terceros (ISO/IEC, 2013).

ISO/IEC 27001: Es el estándar más conocido de la familia proporcionando requisitos para un sistema de gestión de seguridad de la información.

Es adecuada para cualquier organización plantea una mirada completa a la seguridad de la información. Los activos que necesitan protección van de la información digital, documentos en papel y activos físicos (computadoras y redes) a conocimientos de los empleados (ISO/IEC, 2013).

ISO 27001 (Misfud, 2012) lo ayudará a proteger su información en términos de:

(a) Confidencialidad, que asegura la accesibilidad de la información solamente a los que estén autorizados a tener acceso.

(b) Integridad, que protege la precisión y la totalidad de la información y los métodos de procesamiento.

(c) Disponibilidad, que asegura que los usuarios autorizados tengan acceso a la información y activos relacionados cuando se lo exija.

ISO/IEC 27002: Es una guía que proporciona directrices para las normas de seguridad de la información organizacional y las practicas de gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, teniendo en cuenta el(los) entorno(s) del riesgo de seguridad de la información de la organización (ICONTEC, 2015b).

Según ICONTEC (2015b) es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a información contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas: (a) Políticas de la seguridad de la información; (b) Organización de la seguridad de la información; (c) Seguridad del recurso Humano; (d) Gestión de activos; (e) Control de Acceso; (f) Criptografía, (g) Seguridad física y del entorno; (h) Seguridad de las Operaciones; (i) Seguridad de las comunicaciones; (j) Adquisición, desarrollo y mantenimiento de los sistemas; (k)

Relación con los proveedores; (l) Gestión de incidentes de seguridad de la información; (m) Aspectos de seguridad de la información de la gestión de continuidad de negocio; y (n) Cumplimiento.

ISO/IEC 27005: Proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización dando soporte particular a los requisitos de un sistema de gestión de seguridad. Ayudará a las organizaciones en la gestión de riesgos de seguridad de información (ISO/IEC, 2008).

La norma (ISO/IEC, 2008) está diseñada para ayudar a la implementación de la norma ISO / IEC 27001, que se basa en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013, Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de seguridad de la información.

El proceso de gestión del riesgo de seguridad de la información consiste en: (a) Establecimiento contexto; (b) Evaluación de riesgos; (c) Tratamiento de riesgos; (d) Aceptación del riesgo; (e) La comunicación de riesgos; y (f) Seguimiento de riesgos y revisión.

3.2 Seguridad de la Información

La información es un activo más de la organización el cual obtiene un valor nominal, por lo tanto, se debe tratar de una manera estructurada, teniendo en cuenta el estado del arte, el avance tecnológico y estructural conlleva que la información sea vulnerable y esté al alcance de toda persona. Observando la seguridad y el entorno de Ventolini las amenazas se pueden clasificar en dos Parte:

Seguridad Interna: Estas son las que más se presentan dentro de una organización Ventolini no es la excepción principalmente por el desconocimiento de los trabajadores. Ejemplo: fraudes, robo, sabotaje, uso no autorizados de equipos, uso de imagen corporativa sin autorización, desconocimiento del funcionamiento de los equipos o de la infraestructura, corte eléctrico.

Seguridad Externa: violación a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, en esta también podemos clasificar las Naturales las cuales son las ocasionadas por la naturaleza las cuales son: terremotos, avalanchas, inundaciones,

descargas eléctricas, estas no se pueden controlar, pero sí evitar o mitigar.

3.3 Magerit V.3 Metodología de Análisis y Gestión de Riesgos

Metodología que se esfuerza en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente

La Evaluación del riesgo es fundamental para llevar cabo planes de seguridad y de contingencia dentro de la organización, para poder gestionarlos y hacerse riguroso frente a posibles ataques a los datos y la información tanto de la organización, como de los servicios que presta (Gobierno de España, 2012a).

Se compone de tres módulos:

(a) Volumen I Método: aspectos conceptuales y prácticos de la metodología de trabajo

(b) Volumen II Catalogo de elementos: Guía sobre los elementos de metodología.

(c) Volumen III Guía de las técnicas: Guías generales para el análisis de riegos y proyectos de gestión (Análisis costo – Beneficios) (Gobierno de España, 2012a).

Objetivos de Magerit:

a. Directos:

(a) Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

(b) Ofrecer un método sistemático para analizar tales riesgos.

(c) Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

b. Indirectos:

(d) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Magerit persigue los siguientes objetivos (Gobierno de España, 2012b, pp. 7-8):

a. Directos:

(a) Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

(b) Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

(c) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

b. Indirectos:

(a) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos (Gobierno de España, 2012b, pp. 7-8):

(a) Modelo de valor

a. Caracterización del valor que representan los activos para la organización, así como de las dependencias entre los diferentes activos.

b. Mapa de riesgos

c. Relación de las amenazas a que están expuestos los activos.

(b) Declaración de aplicabilidad

a. Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

(c) Evaluación de salvaguardas

a. Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

(d) Estado de riesgo

a. Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar to-mando en consideración las salvaguardas desplegadas.

(e) Informe de insuficiencias

a. Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

(f) Cumplimiento de normativa

a. Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

(g) Plan de seguridad

a. Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

3.4 Modelo de Procesos PHVA

Modelo de Mejoramiento Continuo, El análisis de procesos permite visualizar de una manera completa y sistémica todo el entorno y la singularidad de un proceso determinado, de esta manera se puede realizar una investigación completa relacionada con cada uno de los elementos que componen un proceso o un conjunto de ellos. La filosofía del PHVA es un ciclo en el cual se integran el análisis y la planeación, ya sea para una actividad (De Restrepo, s.f.), procedimiento, o proceso desarrollado, y para optimizar la gestión de estos:

(a) Planificar: se establece la política, objetivos y procesos de calidad necesarios para conseguir resultados de acuerdo con el deseo y capacidad de la organización. En la planeación se definen las metas, y los métodos que permitirán alcanzar el mejoramiento de la calidad.

(b) Hacer: se educa, capacita, y entrena, pero en especial se divulga e implementan los planes y actividades por medio de procesos. Se desarrollan las actividades planeadas y se recopilan datos de la tarea desarrollada.

(c) Verificar: se realiza el seguimiento y la medición de los procesos frente a las políticas, objetivos, planes, metas, requisitos legales y según el nivel de calidad esperado, e informa los resultados, que servirán para la toma de decisiones.

(d) Actuar: se toman decisiones de estandarizar, cuando los procesos satisfacen los requerimientos y objetivos; los que no, se someten a nueva planeación, a acciones correctivas, y/o preventivas, otros procesos demandarán de acciones de mejora continua.

4 METODOLOGÍA

Para alcanzar los objetivos propuestos en esta investigación, el proyecto emplea una investigación de análisis de riesgos que se llevara por etapas.

Una investigación se caracteriza por ser un proceso único de carácter:

a. Sistemático: A partir de la formulación de una hipótesis u objetivo de trabajo, se recogen datos según un plan preestablecido que, una vez analizados e interpretados, modificarán o añadirán nuevos conocimientos a los ya existentes, iniciándose entonces un nuevo ciclo de investigación. La

sistemática empleada en una investigación es la del método científico.

b. Organizado: Todos los miembros de un equipo de investigación deben conocer lo que deben hacer durante todo el estudio, aplicando las mismas definiciones y criterios a todos los participantes y actuando de forma idéntica ante cualquier duda. Para conseguirlo, es imprescindible escribir un protocolo de investigación donde se especifiquen todos los detalles relacionados con el estudio.

c. Objetivo: Las conclusiones obtenidas del estudio no se basan en impresiones subjetivas, sino en hechos que se han observado y medido, y que en su interpretación se evita cualquier prejuicio que los responsables del estudio pudieran hacer.

4.1 Metodología aplicada

Para la gestión de la Seguridad de la información se han tenido en cuenta los requisitos establecidos por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) cual tiene las siguientes normativas:

(a) ISO - IEC 27000 - Vocabulario estándar para el SGSI

(b) NTC - ISO - IEC - 27001- Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

(c) GTC - ISO - IEC - 27002 - *Information technology - Security techniques.* Código de buenas prácticas para la gestión de seguridad de la información.

(d) GTC - ISO - IEC - 27035 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

Para el desarrollo y planificación del análisis de riesgo se ha seguido a:

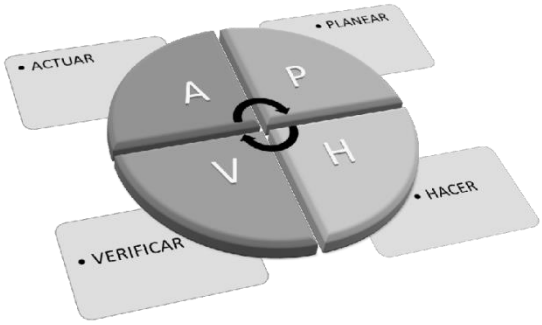
(a) MAGERIT – versión 3.0

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

(b) PHVA - Planificar, hacer, verificar y actuar. En inglés se conoce como PDCA: *Plan*, *Do*, *Check*, *Act.*

Magerit método para analizar los riesgos que soportan los Sistemas de Información y para Recomendar las medidas más apropiadas para mejorar el control. Tiene varias herramientas para ofrecer un mapa de riesgos a que está sujeta Ventolini en el ámbito del proceso.

Se adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, SGSI, como se muestra en la gráfica 1.



Gráfica 1
(M&N ingienería y construcción, 2014)

4.2 Antecedentes

Se realiza el estudio de la temática de seguridad informática en los diferentes diarios y fuentes de información del país, como también los diferentes métodos y estándares de desarrollo para la aplicación de un sistema de gestión de seguridad encontrando lo siguiente:

a. PROTOTIPO PARA LA AUDITORIA SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION (SGSI) – Trabajo de grado realizado por Luisa Fernanda Monphotes Parra y Jose Alexander Alzate Lopez para la Facultad de Ingenierias de la universidad tecnologica de pereira en el año 2014. En donde se desarrolla un prototipo para la gestion de auditorias de seguridad de la informacion con base en la norma ISO/IEC 27001, alli segmenta la auditoria sobre la norma en 4 macrotemas que son: Bases de datos, Inventario, Redes y Seguridad.

b. METODOLOGÍAS PARA AUDITORÍA DE SGSI – Leccion 17 de SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI de la Universidad Nacional abierta y a Distancia (UNAD, s.f.) en donde informan de las normativas acordes a

la norma ISO 27001 que aclaran los procesos para desarrollo de las auditorias a un sistema de gestion de seguridad de la infromacion.

c. MODELO DE SEGURIDAD DE LA INFORMACIÓN – El ministerio de tecnologias de la informacion y las comunicaciones (Ministerio TIC, 2016, p.10)

> El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

5 ESTADO DEL ARTE

De la implementación de procesos para la optimización de seguridad de la información no se tiene conocimiento, como de la infraestructura tecnológica utilizada para ello, ya que esta información no se da a conocer al público es algo que cada empresa se reserva.

De otro lado está la exigencia en la norma ISO/IEC 27001/2013 donde solicita auditorías internas al sistema de gestión ya implementado, lo que hace referencia que la mejor forma de controlar este sistema de gestión son las auditorías internas al sistema (ICONTEC, 2015c).

Por otra parte si se puede contar con la información de los hacking realizados en Colombia para determinar la magnitud, importancia y significado del proceso de

optimización de seguridad para esta empresa.

De allí que en primera instancia se encuentra el posible ataque que se está investigando sobre las elecciones al congreso el 14 de marzo del 2010, cuyo anuncio de publicación fue dado a conocer por el periódico el tiempo cuando informan el 7 de junio del 2011 que "Cámara investigará caso de hackers en la Registraduría" por las elecciones al congreso, pero este es solo un caso de ejemplo, pues día a día se encuentran titulares donde como "Colombia, débil en seguridad informática" (El Tiempo, 2008), demostrando que cada día los líderes de las empresas se dedican a buscar crecimiento y no toman los proyecto del area de sistemas como una buena obra de impacto para asegurar la mantenibilidad y la buena toma de decisiones en una compañía.

CONCLUSIÓN

Como resultado de este trabajo es posible concluir que en el proceso de optimización de seguridad de la información con base en la norma ISO/IEC 27001:2013 para VENTOLINI S.A. en el año 2016, el factor principal es el desarrollo de una auditoría interna, la cual demuestra el estado actual de la compañía y estable las acciones de mejora a seguir para la optimización del sistema de gestión de seguridad de la información.

Conforme a lo anterior y teniendo en cuenta los objetivos de control desarrollados en la norma ISO/IEC 27002 tenemos la gráfica situada en anexos (**anexo 1**).

En la cual encontramos que conforme al estudio de la norma y teniendo en cuenta los 14 Dominios que se especifican en la ISO/IEC 27002 esta empresa tiene solo 2 Controles conforme a la norma, 9 controles que no aplican a la misma, 7 observaciones a los controles aplicados en la misma y 96 no conformidades pues no aplican ningún control con respecto a la norma ó el control no está enfocado a resolver el requerimiento de la norma lo que quiere decir que incumple los requisitos especificados en la misma.

De lo anterior, en Análisis de porcentualidad con respecto a los controles de seguridad solicitados en la norma, esta compañía no cumple en el 84% de los objetivos de controles, y que el 16% de los objetivos de control restantes el 2% son de conformidad a la norma, el 8% no aplica para esta empresa y el 6% tiene observaciones de mejora, como se puede observar en la grafíca 2 (**anexo 2).**

Luego de este estudio, la auditoria exige unos planes donde se establezcan los tiempos para desarrollar las acciones correctivas con respecto a las no conformidades expuestas, por ello es de vital importancia que la compañía realice las siguientes labores:

(a) Realice la implementación de políticas de seguridad de la información y se socialicen.

(b) Realice una revisión periódica de las políticas de seguridad de información.

(c) Realizar campañas de comunicación sobre seguridad de la información para dar a conocer a los empleados de la compañía los riesgos y los procesos implementados por la compañía.

(d) Redactar y dar a conocer los deberes de cada área con sus limitaciones pertinentes.

(e) Estar en contacto con las autoridades pertinentes a la seguridad de la información.

(f) Realizar inscripción a grupos de investigación donde se generen debates con respecto a la seguridad de la información de las compañías.

(g) Generar listado y registro de preguntas para cuando se genera un nuevo proyecto tener en cuenta la seguridad de la información en los mismos.

(h) Realizar cláusulas de seguridad de información para el manejo de equipos móviles de la empresa.

(i) Generar Políticas de trabajo desde casa y asegurar la información que se maneja por medio de un plan de trabajo a distancia.

(j) Generar política de tratamiento de datos para la selección de personal.

(k) Generar Perfiles de trabajo a cada cargo desempeñado en la compañía.

(l) Establecer acuerdos de confidencialidad con los empleados en los contratos laborales de acuerdo a la ley 1581 del 2013.

(m) Informar al empleado sus roles y responsabilidades con respecto a la seguridad de la información.

(n) Implementar control de dominio para administración de seguridad en cada uno de los usuarios.

(o) Generar política de renovación de contraseñas.

(p) Valorizar los activos de información y Documentarlos.

(q) Generar valoración y clasificación de la información administrada por la empresa.

(r) Crear políticas para el manejo de activos fijos.

REFERENCIAS

Alcaldía de Bogotá. (17 de octubre del 2012). Hábeas data. [Ley Estatutaria 1581 del 2012]. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Alzate J. Y Monphothes, L. (2014). *PROTOTIPO PARA LA AUDITORIA SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION (SGSI).* Universidad Tecnológica de Pereira, Colombia

Calder, A. (2006). *Nueve claves para el éxito*. Una visión general de la implementación de la norma NTC-ISO/IEC, 27002.

De Restrepo, J. (s.f.). *PHVA Y LOS SISTEMAS DE GESTIÓN DE LA CALIDAD.* Recuperado en https://sites.google.com/site/emprendimientoinem08/phva-y-los-sistemas-de-gesti%C3%B3n-de-la-calidad

El Tiempo. (2008). *Colombia, débil en seguridad informática.* Periódico El Tiempo. Colombia. Recuperado de http://www.eltiempo.com/archivo/documento/CMS-4393234

El Tiempo. (2011). *Cámara investigará caso de hackers en la Registraduría.* Periódico El Tiempo. Colombia. Recuperado de http://www.eltiempo.com/archivo/documento/CMS-9556404

Gobierno de España. (2012a). *MAGERIT v.3 : 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#.V7DHPZjhC00

Gobierno de España. (2012b). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Informaci*ón. Madrid: Ministerio de Hacienda y Administraciones Publicas.

ICONTEC. (2015a). *NTC-ISO/IEC 27001.* Compendio Seguridad de la Información.

ICONTEC, (2015b), *GTC-ISO/IEC 27002.* Compendio seguridad de la información – segunda edición, pp.1-26

ICONTEC, (2015c), *NTC-ISO/IEC 27001.* Compendio seguridad de la información – segunda edición, p.10

ISO/IEC. (2013). *ISO/IEC 27001: 2013.* Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC. (2008). *ISO/IEC 27005 Will assist organizations in their information security risk managment.* Recuperado de http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1139

ISOTools. (19 de agosto del 2014). *ISO 27001 con los activos de la información de la empresa.* Recuperado en https://www.isotools.org/2014/08/19/iso-27001-activos-informacion-empresa-3/

ISOTools. (15 de enero del 2015). *ISO 27001: Pilares fundamentales de un SGSI.* Recuperado de https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi

Ministerio de Tecnologías de la información y comunicación. (2016). *Modelo de la seguridad y privacidad de la información.* Gobierno de Colombia.

Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

Misfud, E. (2012). *Introducción a la seguridad informática - Seguridad de la información / Seguridad informática.* Gobierno de España. Recuperado de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

M&N ingeniería y construcción. (2014). [gráfica] recuperado de http://myningenieria.com.co/about-us/ciclo-phva/

Semana. (12 de junio del 2015). *¿Qué tan preparado está el gobierno contra ataques cibernéticos?.* Tecnología. Recuperado de http://www.semana.com/tecnologia/articulo/que-tan-preparado-esta-el-gobierno-contra-ataques-ciberneticos/431602-3

UNAD. (s.f.). *6.2 Lección 17 Metodologías para auditoría de SGSI.* Universidad Nacional Abierta y a Distancia, Colombia.

ANEXOS

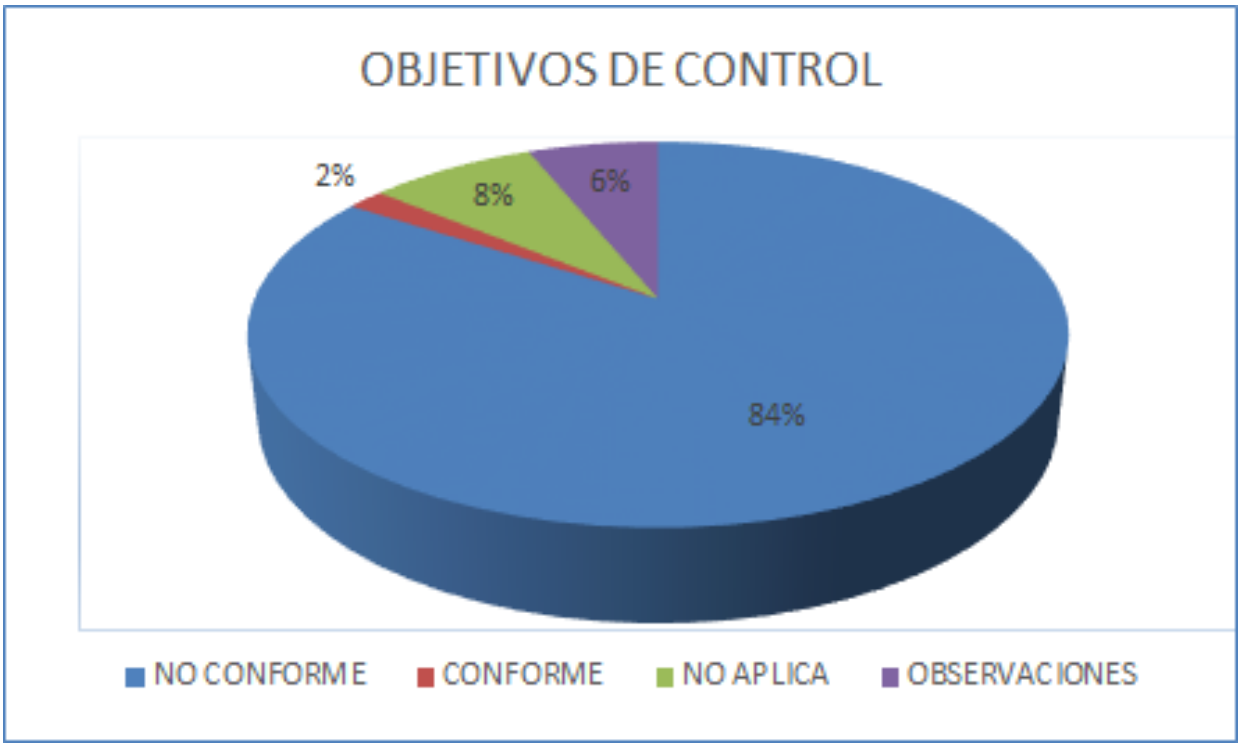
ANEXO 1.

Tabla 1. Objetivos de control desarrollados en la norma ISO/IEC 27002

DESCRIPCION DEL DOMINIO	C	NA	NC	OB	Total general
5			2		2
6		1	6		7
7			5	1	6
8			10		10
9			12	2	14
10			2		2
11			15		15
12		1	10	3	14
13			7		7
14		3	10		13
15		4	1		5
16			7		7
17			4		4
18	2		5	1	8
Total general	**2**	**9**	**96**	**7**	**114**

DESCRIPCION DEL DOMINIO	
05 - POLITICAS DE LA SEGURIDAD DE LA INFOMRACION	C - CONFORMIDAD
06 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	NA - NO APLICA
07 - SEGURIDAD DEL RECURSO HUMANO	NC - NO CONFORMIDAD
08 - GESTION DE ACTIVOS	OB - OBSERVACION
09 - CONTROL DE ACCESO	
10 - CRIPTOGRAFIA	
11 - SEGURIDAD FISICA Y DEL ENTORNO	
12 - SEGURIDAD DE LAS OPERACIONES	
13 - SEGURIDAD DE LAS COMUNICACIONES	
14 - ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
15 - RELACION CON LOS PROVEEDORES	
16 - GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	
17 - ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO	
18 - CUMPLIMIENTO	

ANEXO 2



Grafíco 2. Objetivos de control**.**