ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica
E-ISSN: 2007-5448
recibe@cucei.udg.mx
Universidad de Guadalajara
México

Caiza - Acero, Marcos; Bolaños - Burgos, Francisco
Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador
ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, núm. 3, noviembre-abril, 2014
Universidad de Guadalajara
Guadalajara, México

ReCIBE, Año 3 No.3, Noviembre 2014

Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador

Marcos Caiza-Acero
Facultad de Sistemas, Telecomunicaciones y Electrónica
Universidad Espíritu Santo - Ecuador
mcaiza@uees.edu.ec

Francisco Bolaños-Burgos
Facultad de Sistemas, Telecomunicaciones y Electrónica
Universidad Espíritu Santo - Ecuador
fcobolanos@uees.edu.ec

Resumen: El presente artículo muestra el análisis y la justificación de selección de una de las Normas de seguridad de la información: ISO 27002, COBIT e ITIL para ser implementada en el departamento de sistemas de la Sociedad de Lucha Contra el Cáncer del Ecuador (S.O.L.C.A). El dominio que se analizará es el físico y refleja que el hospital tiene un alto porcentaje de incumplimiento en los controles de protección contra amenzas externas y del medio ambiente así como el de seguridad en la reutilización o eliminación de equipos. Debido a esto, se propone un presupuesto para que se cumplan dichos controles. Finalmente se hacen recomendaciones para que la norma sea implementada en su totalidad en el departamento y luego en la institución.

Palabras claves: SOLCA, normas de seguridad, norma ISO 27002.

The implementations of information security standards: a study of case the Sociedad de Lucha Contra el Cáncer del Ecuador

Abstract: This article shows the analysis and the justification for the selection of one of the information security standards: ISO 27002, COBIT e ITIL to be implemented in the IT department of la Sociedad de Lucha Contra el Cáncer del Ecuador (S.O.L.C.A). The domain to be analyzed is the physical and portrays that the hospital has a high non compliance porcentaje in the controls of protection against external threats and the enviroment as well as the security in the reuse or disposal of equiments. Due to this, a budget is presented in order to comply with this controls. Finally recommendations are given for the implementation of the standard on its overview in the department and later in the institution.

Keywords: SOLCA, information seurity standards, standardISO 27002.

1. Introducción

En la actualidad las tecnologías de la información (TI) han evolucionado a lo largo de la sociedad ecuatoriana, generando múltiples beneficios para grandes y pequeñas organizaciones. Uno de los sectores que se ha beneficiado es el hospitalario, ya que con las TI se ha podido ayudar a muchos pacientes a combatir los tipos de enfermedades que existen en la actualidad. Por tal motivo la seguridad física de los recursos tecnológicos es importante, ya que ayuda a que las historias clínicas de los pacientes estén disponibles en el momento que se requiera y se pueda realizar el respectivo tratamiento (Vidal, García, & Cazes, 2009).

En el caso particular del Hospital de SOLCA, los recursos tecnológicos son una herramienta fundamental para el trabajo diario, porque se necesita visualizar la

información de los pacientes y así poder determinar un tratamiento oncológico específico. (Huayamabe, 2014).

Por lo antes mencionado, es de vital de importancia que el centro hospitalario cuente con la implementación de una norma de seguridad de la información ya que en la actualidad no posee ningún estándar en esta área. Por lo tanto, el objetivo de este paper es mostrar el grado de cumplimiento de la norma seleccionada referente al dominio de la seguridad física. Para luego proponer estrategias con el fin de disminuir el grado de incumplimiento encontrado. Por razones de confidencialidad no se mostrará los antecedentes de la unidad de análisis.

El presente artículo está estructurado de la siguiente manera: La sección 2 es el marco teórico, el cual describe y define las generalidades del tema, la seguridad de la información, la seguridad física y las normas de seguridad. La sección 3 trata el análisis de la caracterización de las metodologías de las normas ISO 27002, COBIT e ITIL y luego justifica la selección de una de ellas. La sección 4 modela la propuesta de implementación que muestra paso a paso la implementación de los controles del dominio físico. La sección 5 cubre el análisis de cumplimiento, donde se propone el presupuesto y un análisis general del cumplimiento de los controles con base en la propuesta de implementación y finalmente en la sección 6 detalla las conclusiones, limitaciones y trabajos futuros.

2. Marco Teórico

2.1 Generalidades

En la actualidad las organizaciones tienen la necesidad de valerse de los sistemas de información, los mismos que son utilizados para almacenar, procesar y distribuir la información, con la finalidad de apoyar a la alta gerencia

a la toma de decisiones. Según Tovar (2009) la información es un conjunto de datos organizados de tal modo que adquiere un valor adicional más allá del propio.

Es por eso que esta se ha convertido en uno de los principales recursos para las compañías, ya sean estas públicas o privadas. Por tal motivo, se enfrenta a una gran variedad de riesgos e inseguridades en los sistemas de información poniendo en peligro la continuidad del negocio. Ante éste escenario es importante que las organizaciones evalúen los riesgos y constituyan estándares y controles adecuados para asegurar la protección de la información. (Areitio, 2008).

Por otro lado es importante tener en cuenta lo fundamental que es la información para las organizaciones y en muchos casos no se le presta la atención necesaria a diferentes sucesos que puedan ocurrir con la información sensible del negocio. Además la globalización de la economía conduce a que esta sea considerada un activo no cuantificado, ya que el intercambio de la misma entre empleados, clientes y proveedores es fundamental para el funcionamiento del negocio. (Carvajal, 2013).

2.2 Seguridad de la Información

La seguridad de la información tiene como objetivo proteger la información de una organización, en cualquier lugar que se encuentre localizada. (Mifsud, 2012) La seguridad de la información tiene cuatro principios fundamentales que son:

Confidencialidad: Previene la divulgación de información no autorizada a personas o sistemas de información. Un ejemplo son los mecanismos criptográficos, que sirven para cifrar o encriptar la información, para que no esté comprensible a aquellos usuarios que no tienen autorización.

Integridad: Garantiza que la información no sea alterada. Un ejemplo son los controles implantados en el software que impiden la duplicidad de la historia clínica de los pacientes.

Disponibilidad: Asegura que el servicio no sea interrumpido. Un ejemplo son los sitios web.

Registro: Crea una evidencia física de los eventos que se dan en un medio informático. Un ejemplo es un log de un firewall.

2.3 Seguridad Física

Lawrence & Butterworth (1997) mencionan que la seguridad física es la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Entre las principales amenazas de un sistema informático están los incendios, terremotos, inundaciones los cuales conllevan a consecuencias catastróficas para la institución. También se presentan amenazas que son ocasionadas por el hombre y estas pueden ser sabotajes internos o externos

La seguridad física también se enfoca en la aplicación de procedimientos de control y barreras físicas, la cual está relacionada con todo el hardware que está siendo utilizado por la institución para el manejo de la información, lo que incluye a los dispositivos conocidos de almacenamiento y medios de acceso remoto. Además otras medidas de seguridad deberán ser evaluadas para su posible implementación de controles de seguridad física de TI para las compañías. (27002, Controles de ISO/IEC, s.f.).

La siguiente figura muestra los parámetros a considerar en la seguridad física de TI según la empresa Business Solutions, compañía líder en integraciones de seguridad.

Figura 1. *Descripción de la Seguridad Física de TI*

Fuente: Monterrey, N.L., México. Soluciones de Tecnología de Información. Global Business Solution empresa especializada en la integración de soluciones de seguridad.

2.4 Normas de seguridad

Según Martinez (2010) las normas son un conjunto de reglas, lineamientos, controles y recomendaciones con el propósito de apoyar los objetivos y políticas de seguridad que son establecidas por la organización. Las normas previenen los riesgos en los accidentes de trabajo mediante órdenes, instrucciones y consignas, que educan al personal que labora en una empresa sobre los diferentes incidentes que pueden suscitarse en el desarrollo de alguna tarea y la manera de prevenir estas situaciones.

Las normas no deben suplantar las diferentes medidas preventivas prioritarias, ya que deben ser un complemento para dichas medidas. Las normas de seguridad se clasifican en dos las cuales son: Normas generales que tienen el objetivo de establecer mecanismos de control para el cumplimiento de objetivos y metas. Normas específicas que tienen el objetivo de establecer mecanismos a alguna operación específica.

3. Análisis de las metodologías.

3.1 ISO 27002

La norma ISO 27002 es un código de buenas prácticas donde se encuentran detallados una serie de controles para la seguridad de la información, además es considerada como una guía para la implementación para un Sistema de Gestión de Seguridad de la Información SGSI. (Instituto Nacional de la Normalización, 2009)

Los dominios que propone ISO 27002 son 11, dentro de esos dominios se encuentran 39 objetivos de control, los mismos que contienen 133 controles. En la Tabla 1 se muestran los dominios de control.

Dominios	**Control**
Política de seguridad.	Proporcionar orientación y apoyo a la alta gerencia para la seguridad de la información, de acuerdo con las leyes actuales.
Organización de la seguridad de información.	Gestionar la información dentro y fuera de la organización
Gestión de activos.	Proteger los activos de la organización.
Seguridad relativa a los recursos humanos.	Asegurar que empleados, contratistas o terceras personas tengan conocimiento de las políticas que tiene la organización.
Seguridad física y del ambiente.	Asegurar las instalaciones de las áreas de procesamiento de información y los recursos tecnológico de la organización.

Gestión de comunicaciones y operaciones.	Asegurar la operación correcta y segura de los medios de procesamiento de información.
Control de acceso	Controlar el acceso a la información
Adquisición, desarrollo y mantenimiento de los sistemas de información.	Asegurar los sistemas de información que tiene la organización
Gestión de incidentes en la seguridad de la información.	Establecer lineamientos para prevenir incidentes de pérdida de información.
Gestión de la continuidad del negocio.	Asegurar que existan planes de continuidad del negocio.
Cumplimiento.	Asegurar el cumplimiento de requisitos legales de seguridad.

Tabla 1. *Resumen de los dominios de control de la norma ISO 27002.*

Fuente: Elaboración propia.

3.2 COBIT

COBIT es una metodología reconocida mundialmente para el control de proyectos de tecnología, los flujos de información y riesgos. El objetivo principal de COBIT es la investigación, el desarrollo y la promoción de un marco de control de gobierno TI actualizado y aceptado a nivel mundial, para que las empresas adopten sus beneficios y sea utilizado por la alta gerencia del negocio, profesionales de TI y expertos en seguridad informática. (IT Governance Institute, 2007) En la Tabla 2 se muestra las características que menciona COBIT.

Características	**Objetivos**
Orientado a negocios.	Proporciona la información que la organización requiere para alcanzar los objetivos.
Orientado a procesos.	Ofrece un modelo de procesos y un lenguaje común para todas las personas que integran la organización.
Basado en controles.	Proveen de un conjunto de requerimientos de alto nivel, que son considerados por la alta gerencia para un efectivo control.
Impulsado por mediciones.	Comprender el estado de los sistemas de TI que tienen en la actualidad.

Tabla 2. *Caracteristicas de COBIT*

Fuente: Elaboración propia.

3.3 ITIL

ITIL V3 es una metodología ordenada al momento de plantear la prestación de servicios de TI y establece la estructura a utilizar en la mayoría de organizaciones que se identifican con las buenas prácticas de gestión de servicios. ITIL también es conocida como una recopilación de libros con base en las mejores prácticas en las organizaciones de éxito actual. (Kolthof, de Jong, & Van Bon, 2008)

En la Tabla 3 ITIL V3 plantea un enfoque de cinco fases de su ciclo de vida para la gestión de los servicios de TI.

Características	Objetivos
Estrategias de servicio.	Diseño, desarrollo e implementación se ajusten a políticas del negocio.
Diseño del servicio.	Diseñar y desarrollar los servicios que son necesarios para la organización.
Transición del servicio.	Gestionar y coordinar los sistemas, procesos y funciones que son necesarios para la creación, comprobación e implantación de los nuevos servicios del negocio.
Operaciones de servicio	Coordinar las actividades y procesos que son importantes para la gestión de servicios de los usuarios y clientes de la organización.
Mejora continua	Mejorar los servicios de manera que garantice el cumplimiento de las necesidades de la organización.

Tabla 3. *Resumen de los dominios de ITIL.*

Fuente: Elaboración propia.

3.4 Selección y justificación de la metodología

La metodología a implementarse es la de la norma ISO 27002, debido a que contiene un marco teórico de trabajo para la gestión de seguridad de la información y dentro de esta existe un dominio de seguridad física y del ambiente. Además SOLCA cuenta con la certificación ISO 9001, de esta manera se estaría siguiendo los lineamientos de certificación de la casa de salud.

A continuación se muestra en la Tabla4 un cuadro comparativo entre las metodologías COBIT 4.1, ITIL v3 e ISO 27002 que se realizó para la selección de la metodología a utilizar.

ÁREAS CLAVES	COBIT	ITIL	ISO 27002
FUNCIONES	Mapeo de procesos.	Mapeo de gestión de niveles de servicio de TI.	Marco de referencia de seguridad de información.
OBJETIVO	Brindar buenas prácticas a través de un marco de trabajo.	Proporcionar herramientas que mejoren la calidad de los servicios.	Proporciones mejores prácticas en la seguridad de la información.
ÁREAS	4 procesos y 34 dominios.	9 procesos.	11 dominios y 133 procesos.
CREADOR	Information systems audit and control association. (ISACA)	Office of Government Commerce. (OGC)	International Organization for Standardization. (ISO)
¿PARA QUÉ SE IMPLEMENTA?	Auditoría de sistemas de información.	Gestión de niveles de servicio.	Cumplimiento de los estándares de seguridad
¿QUIÉNES LO EVALUAN?	Compañías de contabilidad, de auditoria o de consultoría de TI.	Compañías de consultoría de TI.	Compañías de seguridad en redes, de consultoría de TI y empresas de seguridad.
BENEFICIOS	Apoyar las decisiones, alcanzar los objetivos estratégicos,	Satisface a usuarios, mejora comunicación entre áreas, clarifica los roles	Brinda una metodología para la gestión de seguridad, se da confianza a clientes,

	optimizar los servicios y obtener los beneficios del negocio deseado.	de la organización.	ayuda a identificar y mejorar las áreas débiles.

Tabla 4. *Cuadro Comparativo de Metodologías COBIT 4.1, ITIL V3 e ISO 27002.*

Fuente: Elaboración propia. Asdaptado de Alineando COBIT 4.1, ITIL V3 e ISO 27002 para beneficio del negocio. (Valero, sf)

4. Propuesta de implementación de la norma ISO 27002.

El dominio de control que se aplicará es el de la seguridad física y del ambiente. Ciertos controles no se implementarán debido a que el departamento cumple con los mismos o están fuera de sus funciones. En la Figura 2 se muestra la distribución de las oficinas del centro de cómputo, donde se va a implementar los controles de seguridad física.

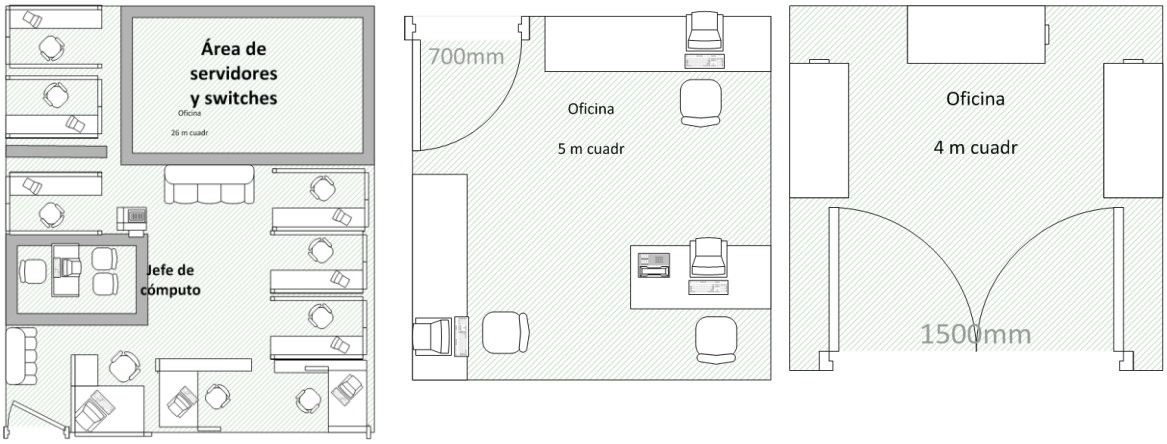

Figura 2. *Distribución del centro de cómputo.*
Fuente: Elaboración propia.

4.1 Implementación de las áreas seguras

4.1.1 Perímetro de seguridad física.

Los numerales d y e no son tomados en consideración para la implementación de éste control. Se deben de implementar las siguientes recomendaciones:

a. Se debe definir la ubicación y resistencia del perímetro de seguridad de las instalaciones del centro de cómputo.
b. Se deberá instalar tres cerraduras electromagnéticas y tres lectores de tarjetas de seguridad para las puertas de ingreso a las instalaciones del departamento de cómputo con la finalidad de controlar el acceso no autorizado de terceras personas.
c. La institución debe asignar un guardia de seguridad para controlar el acceso físico a las instalaciones del departamento de cómputo.
d. Dentro del departamento de cómputo se deberá instalar tres alarmas y tres sistemas de circuito cerrado de TV, para la detección de intrusos.
e. Las áreas médicas deben estar separadas físicamente de las instalaciones del departamento de cómputo.

4.1.2 Controles de acceso físico.

El numeral e no se considera en la implementación de este control. Se deben de implementar las siguientes recomendaciones:

a. El guardia de seguridad debe registrar la hora y fecha de entrada de visitantes, contratistas o cualquier personal que no pertenezca al área y que estén debidamente autorizado el ingreso a las instalaciones del departamento de cómputo.
b. Se deberá instalar una cerradura biométrica para acceder al área de servidores.
c. La institución debe de proveer al guardia de seguridad de diez tarjetas de identificación para visitantes y contratistas, los mismos que deben presentar una identificación al momento de ingresar a las instalaciones del departamento de cómputo.
d. Se deberá llevar un registro de fecha, hora y quién autoriza el ingreso para todo personal ya sea interno y/o externo al área de servidores. Este registro lo debe hacer una persona del área de Producción o alguien que sea asignado por el jefe de cómputo.

4.1.3 Seguridad de oficinas, despachos e instalaciones.

Los numerales b, c y d no son tomados en consideración para la implementación de éste control. Se debe implementar la siguiente recomendación:

a. El departamento de cómputo debe considerar las regulaciones y procedimientos que proporciona el ministerio de relaciones laborales en referencia al reglamento de seguridad y salud de los trabajadores y mejoramiento del medio ambiente del trabajo. (Ministerio de Relaciones Laborales, 2012)

4.1.4 Protección contra amenazas externas y del ambiente

Todos los numerales de éste control son considerados para la implementación del control. Se deben de implementar las siguientes recomendaciones:

a. Se deberá almacenar en la bodega de cómputo los recursos tecnológicos y suministros de oficina.
b. La institución deberá asignar una nueva área para la creación de un departamento de cómputo alterno.
c. Se deberá instalar tres equipos apropiados contra incendio y su respectiva señalización para las instalaciones del departamento de cómputo.

4.1.5 El trabajo en las áreas seguras.

Los numerales a, b y c no son tomados en consideración para la implementación de éste control. Se deben de implementar las siguientes recomendaciones:

d. Se deberá prohibir el uso de equipos de fotografía, audio y video dentro de las áreas del departamento de cómputo, salvo alguna autorización de la alta gerencia o del jefe de cómputo.

4.1.6 Áreas de acceso público, de entrega y de carga

Este control no será implementado, debido a que no corresponde a las funciones del centro de cómputo.

4.2 Implementación de la seguridad del equipamiento

4.2.1 Ubicación y protección del equipamiento.

Los numerales a, b, c, d y i no son tomados en consideración para la implementación de éste control. Se deben de implementar las siguientes recomendaciones:

e. Se deberá pegar tres juegos de afiches en lugares estratégicos para la prohibición de comer, fumar y beber dentro de las instalaciones del departamento de cómputo.
f. Se deberá adquirir un equipo para la medición de temperatura y humedad dentro de las instalaciones del departamento de cómputo.
g. Se deberá instalar un pararrayo en el edificio donde se encuentra ubicado las instalaciones del departamento de cómputo.
h. Se deberá adquirir trece paquetes de cobertores para todo el equipamiento de TI que se encuentre dentro de las instalaciones del departamento de cómputo.

4.2.2 Elementos de soporte.

Este control no será implementado, debido a que no corresponde a las funciones del centro de cómputo.

4.2.3 Seguridad en el cableado.

Los numerales a, b, c, d, e y f cumplen con los objetivos de implementación de éste control.

4.2.4 Mantenimiento del equipo.

El numeral b no es tomado en consideración para la implementación de éste control. Se deben realizar las siguientes consideraciones para el mantenimiento de equipo:

a. Los suministros de las impresoras deben ser originales, tal como lo recomienda el proveedor.
c. Se deberá desarrollar un módulo dentro del sistema para el registro de todas las fallas de los equipos de TI, así como el mantenimiento correctivo y preventivo de las instalaciones del departamento de cómputo.
d. Se deberá elaborar un acta de consentimiento al momento de retirar y entregar el equipamiento de TI, a fin de evitar la pérdida de información o mal uso del activo.
e. Se debe cumplir con las condiciones que imponen las de pólizas de seguros para los equipos de TI de las instalaciones del departamento de cómputo.

4.2.5 Seguridad del equipamiento fuera de las instalaciones de la organización.

Los numerales a, b y c, no son tomados en consideración para la implementación de éste control. Se deben de implementar la siguiente recomendación:

d. Se deberá adquirir una póliza de seguro para los equipos de TI que se consideren necesarios para las instalaciones del departamento de cómputo.

4.2.6 Seguridad en la reutilización o eliminación de los equipos.

Se deben de implementar la siguiente recomendación:

a. Se deberá adquirir un software para asegurar la correcta eliminación de la información.

Existen software gratuito que realiza la función de eliminación segura de la información.

4.2.7 Retiro de bienes.

Los numerales a, b y d, no son tomados en consideración para la implementación de éste control. Se deben de implementar la siguiente recomendación:

c. Se deberá agregar un reporte en el sistema de retiro de equipamiento, para controlar el tiempo que lleva fuera de las instalaciones y comprobar el cumplimento de su regreso.

5. Análisis del cumplimiento de la implementación de la norma ISO 27002.

5.1 Presupuesto

Una vez concluida la implementación de controles para la seguridad física de los recursos tecnológicos del departamento de cómputo del hospital de SOLCA, se procede a dar a conocer los costos referenciales, tomando en consideración que

se trata de una institución privada sin fines de lucro. En la Tabla 5 se considera todos los rubros que son utilizados para mejorar la seguridad en la institución con base en la implementación de la norma ISO 27002.

N ° DE CONTROL	DESCRIPCIÓN DEL CONTROL	CANTIDAD	PRECIO UNITARIO	TOTAL
1	Servicio profesional de la propuesta de implementación	1	3000	3000
2	Cerraduras electromagnéticas.	3	150	450
3	Cerradura biométrica.	1	340	340
4	Tarjetas de seguridad.	180	540	
5	Alarma contra intrusos.	3	200	600
6	Circuito cerrado de TV.	3	500	1500
7	Guardia de seguridad.	1	600	600
8	Tarjetas de identificación visitantes.	10	5	50
9	Cuadernos de registros.	2	5	10
10	Construcción de un centro de cómputo alterno.	1	12000	12000
11	Equipos contra incendio.	3	300	900
12	Cableado de equipo contra incendio.	1	350	350
13	Señalización de lo que está prohibido.	3	50	150
14	Equipos de medición de temperatura y humedad.	3	50	150
15	Pararrayo	1	600	600
16	Cobertores de equipos de TI.	13	10	130
17	Póliza de seguros para los recursos tecnológicos.	1	700	700
			TOTAL	$22,070

Tabla 5. *Costo Referencial de la Implementación en dólares Estado Unidenses.*

Fuente: Elaboración propia. Asdaptado de Alineando COBIT 4.1, ITIL V3 e ISO 27002 para beneficio del negocio. (Valero, sf)

5.2 Análisis de la seguridad física actual con base en la implementación de la norma.

En éste punto se puede concluir que la situación actual del departamento de cómputo con relación a la seguridad física, no cumple con algunos procedimientos de control de seguridad que establece la norma ISO 27002 y es necesario implementarlos, para que satisfagan las necesidades de la institución, ya que su costo no es muy elevado en comparación de lo que se perdería si llegase a ocurrir algún tipo de incidente dentro de las instalaciones del centro de cómputo. (Calder, 2009)

En la Figura 3 se muestra el cumplimiento de cada control del dominio de seguridad física que menciona la norma sobre la situación actual de la institución.

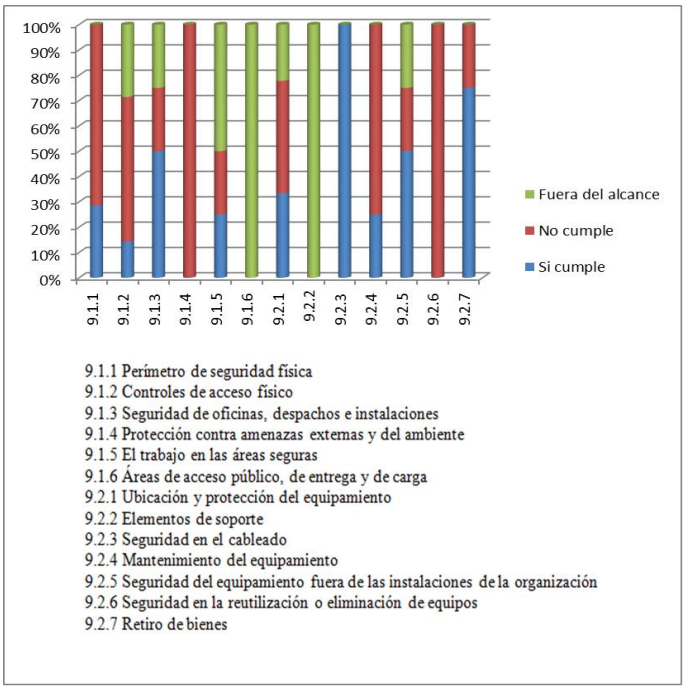

Figura 3. *Cumplimiento del dominio de seguridad física y del ambiente.*

Fuente: Elaboración propia.

Con base en la figura anterior se puede concluir que los controles que no implementan ningún tipo de medida de seguridad son: el de protección contra amenzas externas y del medio ambiente así como el de seguridad en la reutilización o eliminación de equipos. Otros controles que muestran un alto porcentaje de no cumplimiento con relación a la norma son: el perímetro de seguridad fisica, el control de acceso, la ubicación y protección de equipamiento y el mantenimiento del equipo.

6. Conclusiones

En la sección anterior se puede apreciar el grado de cumplimiento de los dominios de la norma ISO 27002. Por lo tanto los tipos de amenazas a los que están expuestos los recursos informáticos son: instalaciones inadecuadas para el equipamiento de TI, ausencia de equipos para combatir incendios, robos, accidentes laborales, destrucción intencional o desastres naturales y la ausencia de mecanismos para la identificación del personal interno o externo al departamento. Con esto se evidencia la necesidad de implementar el estándar a la brevedad posible debido a la información sensible que la casa de salud maneja.

El presente trabajo tiene las siguientes limitaciones: La implementación de la norma en su totalidad ya que falta analizar los otros 10 dominios descritos en la Tabla #1. La carencia de un espacio físico para reubicar al departamento de sistemas ya que en la actualidad se encuentra cerca de una zona que no recomienda la norma. Y por último la falta de roles y de personal en el departamento de cómputo.

Los trabajos futuros con base en este estudio son: Aplicar los demás dominios de control que menciona la norma ISO 27002 al departamento de sistemas ya que así se contará con la implementación de la misma en su totalidad, garantizando la protección de la información en todas las áreas y obteniendo la

certificación pertinente. Implementar el mismo dominio en los departamentos de laboratorio clínico, anatomía patológica, emergencia, consulta externa, preadmisión, radio oncología, oncología clínica y radiología teniendo como guía el procedimiento usado aplicando las variantes respectivas. Por último definir un plan y el comité de contingencias ya que def esta manera se pueda establecer de forma clara los procedimientos a seguir y las responsabilidades de cada miembro ante posibles desastres en el departamento de cómputo.

Bibliografía

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Paraninfo.

Calder, A. (2009). Implementing Information Security Based on ISO 27001/ISO 27002.

Carvajal, A. (2013). Fundamentos de la inseguridad de la información. Académia Española.

Huayamabe, M. (04 de 2014). Seguridad física del centro de cómputo. (M. Caiza, Entrevistador)

Instituto Nacional de la Normalización. (2009). Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información .

IT Governance Institute. (2007). COBIT 4.1. Obtenido de http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

IT Governance Institute. (s.f.). Alineando Cobit 4.1, Itil V3 e ISO/IEC 27002 en beneficio del negocio. Recuperado el 20 de mayo de 2013, de http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

Kolthof, A., de Jong, A., & Van Bon, J. (2008). Fundamentos de la Gestión de Servicios de IT Basada en ITIL®V3.

Lawrence , F., & Butterworth, H. (1997). Effective Physical Security.

Martinez, A. (2010). Manual de normas y politicas de seguridad informatica aplicado a la Universidad de Oriente.

Mifsud, E. (2012). Introducción a la seguridad informática. Obtenido de http://files.formatv.webnode.es/200000063-1ac031cb4d/SEGURIDAD%20INFORMATIVA.pdf

Ministerio de Relaciones Laborales. (2012). REGLAMENTO DE SEGURIDAD Y SALUD DE LOS TRABAJADORES Y MEJORAMIENTO DEL MEDIO AMBIENTE DE TRABAJO. Obtenido de http://www.relacioneslaborales.gob.ec/wp-content/uploads/downloads/2012/12/Reglamento-de-Seguridad-y-Salud-de-los-Trabajadores-y-Mejoramiento-del-Medio-Ambiente-de-Trabajo-Decreto-Ejecutivo-2393.pdf

Paucar, E. (29 de 07 de 2011). Los pacientes saturan las salas de Solca.

SOCIEDAD DE LUCHA CONTRA EL CANCER DEL ECUADOR. (s.f.). Recuperado el 20 de 11 de 2013, de www.solca.med.ec

Tovar, M. (2009). Las tecnológias de la información y las comunicación para la documentación. Obtenido de http://www.ugr.es/~eues/webgrupo/Docencia/TovarDiaz/SistemasInformaticos/tema1Sist.pdf

Valero, F. (sf). Alineando CobiT 4.1, ITIL V3 e ISO 27002 para beneficio del negocio. Obtenido de http://www.binaryti.com/2011/12/alineando-cobit-41-itil-v3-e-iso-27002.html

Vidal, L., García, L., & Cazes, T. (14 de 12 de 2009). Seguridad, Información y Salud. Obtenido de http://www.rcim.sld.cu/revista_7/articulo_htm/segurinfsalud.

Notas biográficas:

Marcos Caiza Acero Ingeniero en Sistemas con concentración en Consultoría de Sistemas por la Universidad de Especialidades Espíritu Santo (Ecuador, 2014). Actualmente labora en la Sociedad de Lucha Contra el Cáncer del Ecuador en el Departamento de Cómputo.

Francisco Bolaños Burgos Ingeniero en Computación Especialización Sistemas de Información y Magíster en Seguridad Informática Aplicada de la

Escuela Superior Politécnica del Litoral. Profesor a tiempo completo en la Facultad de Sistemas Telecomunicaciones y Electrónica de la Universidad de Especialidades Espíritu Santo. Cátedras impartidas: Sistemas operativos, sistemas distribuidos, Ethical hacking, seguridad de redes, ecommerce y new technologies. Área de investigación: computación forense, criptografía y comercio electrónico.