ESTUDIO DEL ESTÁNDAR PARA LA SEGURIDAD DE LA INFORMACIÓN ISO 27002 Y SU COMPARACIÓN CON LOS ESTÁNDARES ISO 27001, COBIT Y OSSTMM

OSCAR FERNANDO GONZALEZ FLOREZ

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
Facultad de Ingeniería de Sistemas
Bucaramanga, Colombia
2013

ESTUDIO DEL ESTÁNDAR PARA LA SEGURIDAD DE LA INFORMACIÓN ISO 27002 Y SU COMPARACIÓN CON LOS ESTÁNDARES ISO 27001, COBIT Y OSSTMM

OSCAR FERNANDO GONZALEZ FLOREZ
COD. 33197030

Trabajo de grado elaborado como requisito para optar por el título de:
Ingeniero de Sistemas

Director
Msc. ROBERTO CARVAJAL SALAMANCA

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA UNAB
Facultad de Ingeniería de Sistemas
Bucaramanga, Colombia
2013

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bucaramanga, 2013

DEDICATORIA

Un agradecimiento especial al Director Mc. ROBERTO CARVAJAL SALAMANCA Director del Proyecto, quien me permitió, después de un largo receso académico, retomar los conocimientos acumulados durante mi carrera profesional y aplicarlos en el desarrollo de éste Proyecto de grado, que espero pueda servir de referente para futuras generaciones. Así mismo, reconozco la labor de los docentes, compañeros, tutores y de aquellas personas, que de una u otra forma, y durante tantos años, aportaron elementos valiosos para alcanzar este nuevo peldaño.

AGRADECIMIENTOS

Dedico este nuevo logro a mi familia, a mi esposa, y especialmente a mi hijo Jonás, quien viene en camino, y quien me inspiró y se convirtió en mi más fuerte motivación para terminar mi carrera y convertirme en profesional, enseñándome que siempre habrá una razón para continuar y que nunca es tarde para alcanzar las metas propuestas.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Resumen del Estándar Internacional ISO/IEC 27002

El Estándar Internacional ISO/IEC 27002 nace bajo la coordinación de dos organizaciones:

- ISO: International Organization for Standardization.
- IEC: International Electrotechnical Commission.

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información, que es en esencia de lo que trata el Estándar Internacional ISO/IEC 27002 (antiguamente llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002).

El ISO/IEC 27002 se refiere a una serie de aspectos sobre la seguridad de de las tecnologías de información, entre los que se destacan los siguientes puntos:

- Evaluación de los riesgos de de seguridad: se deben identificar, cuantificar y priorizar los riesgos.
- Política de seguridad: deben haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.
- Aspectos organizativos de la seguridad de la información: cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.)
- Gestión de activos: se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

- Seguridad ligada a los recursos humanos: especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

- Seguridad física y ambiental: consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

- Gestión de comunicaciones y operaciones: asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

- Control de acceso: deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

- Gestión de incidentes en la seguridad de la información: los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer, etc.

- Gestión de la continuidad del negocio: se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

- Cumplimiento: debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc.

INTRODUCCIÓN

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. El continuo flujo de información y su traslado de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y por tanto toda la información que en ella se contiene. Actualmente la implantación de controles y procedimientos de seguridad se realiza frecuentemente sin un criterio común establecido, centrado en la adquisición de productos de carácter técnico y sin tener en cuenta la protección de la información. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

Este proyecto busca generar un prototipo de una herramienta que apoye la gestión de controles de seguridad de la información, tomando como estándar ISO 27002.

1. ESTADO DEL ARTE

Las organizaciones que requieren implementar una estrategia de seguridad para proteger su información bajo los estándares internacionales, deben desarrollar e implantar un SGSI (sistema de gestión de seguridad de la información). Este proceso de administración y certificación de seguridad se debe hacer según normas como la ISO/IEC 27002, ISO/IEC27001, COBIT u OSSTMM. Su primera versión sale en el año de 1995 como recomendaciones para seguridad basadas en las mejores prácticas llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002 siendo un estándar certificable aceptado actualmente por el ICONTEC en Colombia.

El ISO/IEC 27002 se refiere a una serie de aspectos sobre la seguridad de las tecnologías de información, estableciendo diez dominios de control que cubren por completo la gestión de la seguridad de la información:

Política de seguridad: deben haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.

Organización de la seguridad: cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.)

Gestión de activos: se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

Seguridad ligada a los recursos humanos: especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

Seguridad física y ambiental: consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

Administración de comunicaciones y operaciones: asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

Control de acceso: deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

Adquisición, desarrollo y mantenimiento de los sistemas de información: consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

Gestión de la continuidad del negocio: se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

Cumplimiento de la normatividad legal: debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc.

Cada dominio busca cumplir con unos objetivos que suman 56 en total. Para cumplir los objetivos se deben evaluar 127 controles que son las recomendaciones de la norma, las organizaciones deciden si adoptar o no el control dependiendo del nivel de seguridad que desean para sus activos informáticos.

En el contexto internacional existen modelos estandarizados para buenas prácticas de seguridad como ISO 27002, OSSTMM, COBIT, entre otros y mecanismos basados en software para implantación de SGSI; estos son muy globales y genéricos. Algunos como:

GxSGSI - SOFTWARE DE ANALISIS DE RIESGOS[1]: El programa 'GxSGSI' es - según responsables de AENOR - una herramienta que automatiza el Análisis y

[1] Disponible en Internet: http://www.b2bi.es/plantilla_detallenoticia.php?IDNOTICIA=66

Gestión de los Riesgos, de una manera rápida, completamente parametrizable y eficaz.

Este programa, desarrollado íntegramente por la entidad asturiana SIGEA, incorpora en su versión básica módulos que permiten realizar de manera fácil e intuitiva tareas relacionadas con el inventario de Activos, Amenazas, Vulnerabilidades y Riesgos. Selección de Controles y Gestión de Incidencias, entre otras.

GlobalSGSI[2]: GlobalSGSI es la herramienta web que facilita la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información conforme a la norma ISO 27001.Permite mantener su sistema mediante la automatización de los procedimientos y planes que establece el estándar ISO 27001.

Dispone de módulos para la gestión de incidencias, auditorías, formación, capacitación, continuidad de negocio, etc.

E-Pulpo[3]:E-PULPO es una plataforma que cubre las necesidades de gestión de la seguridad de la información en las organizaciones, tanto en la Administración Pública como el sector privado: Esquema Nacional de Seguridad (ENS), LOPD, SGSI (ISO 27001), etc.

E-PULPO es el resultado de la integración de aplicaciones open source para dar cobertura a todos los procesos organizativos alrededor de la seguridad. Su integración con la herramienta EAR/PILAR la convierte en la solución ideal para la adecuación al Esquema Nacional de Seguridad (ENS).

Meycor COBIT Autoevaluación de Controles - Control Self-Assessment (CSA)[4]: El software MEYCOR COBIT (CSA) ha sido desarrollado por DATASEC y constituye una herramienta con características únicas a nivel mundial, ya que en su versión actual, se encuentran incorporados estándares mundiales como el marco COBIT® 4.1. Esta herramienta ha tenido una evolución constante desde su primera versión. La evolución es producto de la incorporación de nuevos

[2] Disponible en Internet: http://www.globalsgsi.com/de-un-vistazo
[3] Disponible en Internet: http://www.globalsgsi.com/de-un-vistazo https://www.e-pulpo.es/
[4] Disponible en Internet: http://www.datasec-soft.com/sp/content/view/7/12/

elementos que posibilitan la evaluación de múltiples centros de análisis o el seguimiento de varios períodos de evaluación.

Secuware Security Framework (SSF)[5]: Secuware Security Framework (SSF) es la suite empresarial modular para proteger la información de la empresa en el puesto de trabajo, independientemente del lugar o del medio de almacenamiento empleado.

Creado como suite integrada con sistema operativo de seguridad propio y gestión centralizada, Secuware Security Framework aporta las funcionalidades de seguridad multinivel que requieren las corporaciones para garantizar la confiabilidad y el cumplimiento de las políticas. Las empresas pueden optar por desplegar desde un único producto hasta la suite completa.

También podemos encontrar trabajos relacionados con ISO/IEC 27002 como el trabajo klaic (2011), Horváth (2009), Iqbal (2009); en los cuales se hace análisis del uso de la norma.

En el contexto regional y nacional, son escasos los antecedentes de herramientas de administración de información de controles de seguridad informática. Según ACIS "Más del 66% de las empresas en Colombia no cuentan con una política de seguridad definida formalmente" y"Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de seguridad de la información…". Por su lado, el Ministerio de Comunicaciones a través del Plan nacional de TIC Colombia 2010-2019, también contempla la relevancia del sector de la seguridad informática, donde plantea la asignación de recursos para invertir en el Proyecto "Seguridad informática para el sector público y privado" cuyo objetivo es "Establecer lineamientos generales y prácticos en los temas de seguridad de la información desde la perspectiva del ciudadano; de la experiencia técnica y administrativa de las organizaciones, los estándares y las buenas prácticas; y de la protección de infraestructura crítica de la nación"[6] . Lo cual evidencia también la necesidad de desarrollar trabajos desde el sector investigativo en ésta área.

[5] ACIS (Asociación Colombiana de Ingenieros de sistemas) - Investigación - Encuesta nacional Seguridad informática en Colombia: Tendencias 2010. Msc. Andrés Almanza - Ph.D. Jeimy J.Cano, Disponible en Internet. [http://www.acis.org.co/fileadmin/Revista_115/investigacion.pdf]

[6] Ministerio de Comunicaciones – Plan Nacional de TIC´s 2010-2019 Disponible en Internet: http://www.colombiaplantic.org/docs/080409-Plan%20Nacional%20de%20TIC.pdf

Tabla 1. Cuadro Comparativo de Herramientas SGSI

CUADRO COMPARATIVO DE HERRAMIENTAS SGSI					
HERRAMIENTA / CARACTERISTICA	GXSGSI	GLOBAL SGSI	E-PULPO	MEYCOR COBIT KP	SECUWARE SECURITY
Creador	SIGEA	AUDISEC	INGENIA	DATASEC	SECUWARE
Sistemas operativo	WINDOWS XP/VISTA/2000/2003	WINDOWS XP/VISTA/2000/2003	INSTALADO EN UN APPLIANCE HARDWARE PLATAFORMA VIRTUAL CLOUD INGENIA	WINDOWS XP/VISTA/WINDOWS 7/2000/SERVER 2003-2008	WINDOWS XP/VISTA/2000 ADMINISTRACIÓN: WINDOWS 2000 PROFESIONAL Y SERVER/XP/2003 SERVER
Licencia	COMERCIAL	COMERCIAL	GNU GPL V2	COMERCIAL	COMERCIAL
Estándares Incluidos	UNE 71502 – ISO 27001	ISO27001	ITIL-LOPD-ENS-ISO27001-ISO27002-ISO20000	ISO27001-COBIT-ISO27002-ISO20000-COSO I-COSOII	NINGUNO (SUITE EMPRESARIAL)
Gestión Documental	-	X	X	X	-
Gestión de Incidencias	X	X	X	X	-
Autoevaluación	-	X	-	X	-

2. MARCO TEÓRICO

2.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN[7]

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Es la herramienta de la cual dispone la dirección para llevar a cabo las políticas y los objetivos de seguridad, corresponde a un proceso sistemático, documentado y conocido por toda la organización para garantizar que la seguridad de la información es gestionada correctamente: las organizaciones deben demostrar que identifican y detectan los riesgos a los que está sometida y que adoptan medidas adecuadas y proporcionadas.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

[7] Disponible en Internet: http://www.iso27000.es/sgsi.html#section2a

¿PARA QUE SIRVE UN SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

Figura 1. Estructura global de un SGSI

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

¿COMO SE IMPLEMENTA UN SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

Plan (planificar): establecer el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorizar y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI.

Plan: Establecer el SGSI

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Definir una política de seguridad que:

- Incluya el marco general y los objetivos de seguridad de la información de la organización;

- Considere requerimientos legales o contractuales relativos a la seguridad de la información;

- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

- Establezca los criterios con los que se va a evaluar el riesgo;

- Esté aprobada por la dirección.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

Identificar los riesgos:

- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

- Identificar las amenazas en relación a los activos;

- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

- Estimar los niveles de riesgo;

- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- Aplicar controles adecuados;
- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
- Transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

Figura 2. Gestión de Riesgos

Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

- Definir una declaración de aplicabilidad que incluya:
- Los objetivos de control y controles seleccionados y los motivos para su elección;

- Los objetivos de control y controles que actualmente ya están implantados;

- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

- Gestionar las operaciones del SGSI.

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

La organización deberá:

Ejecutar procedimientos de monitorización y revisión para:

- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;

- Identificar brechas e incidentes de seguridad;

- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la claúsula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

2.2 LA SERIE ISO/IEC 27000[8]

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo-por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Historia y Evolución del estándar ISO/IEC
Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001
1992 Publicación BS 7750 - ahora ISO 14001
1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

[8] Disponible en Internet: http://www.iso27000.es/sgsi.html#section2a

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Figura 3. Evolución de ISO 27000

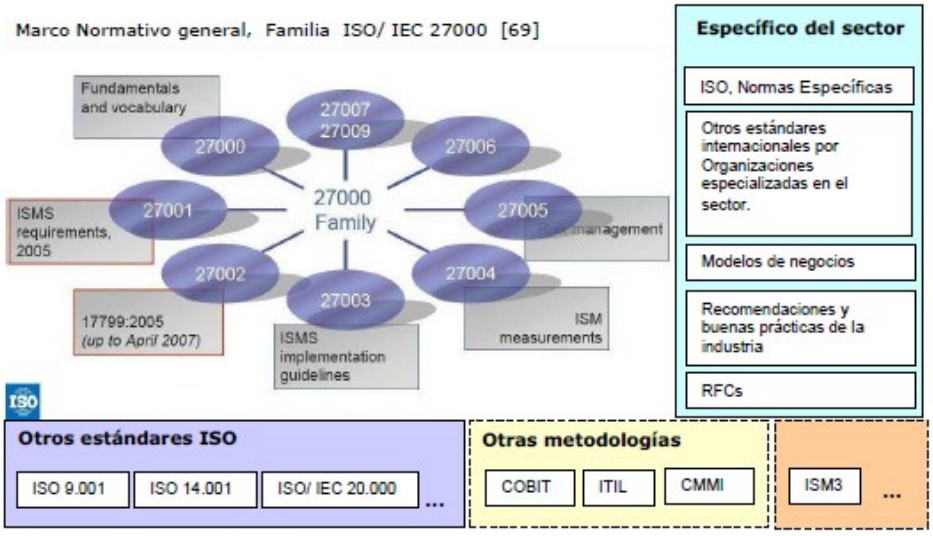
En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

CONTEXTO NORMATIVO – ESTANDARES

En la Figura 4 se ilustra el marco normativo de los diferentes estándares que, de una u otra manera, están vinculados a un Sistema de Gestión de la Seguridad de la Información.

En él se ven representados estándares internacionales de diferente naturaleza y con diferente alcance. Algunos de ellos, como por ejemplo la serie ISO/IEC 27.000 e ISM3, son específicos de la gestión de seguridad de la información, generales y aplicables a cualquier sector de actividad. Pero también deben tenerse en cuenta otros estándares y recomendaciones que son específicas del sector. Incluso puede existir la necesidad de alinear más de un estándar, como por ejemplo ITIL con la familia ISO/IEC 27.000, o de esta última con la ISO 9001, por citar otro ejemplo**.**

Figura 4. Contexto Normativo de un SGSI



Un SGSI, como sistema de gestión que es, de una disciplina específica como lo es la seguridad de la información, debe relacionarse con otros sistemas de gestión, por ejemplo de Gestión de Calidad entre otros. Es así que también deben considerarse en el contexto, estos otros sistemas y los respectivos estándares metodológicos en los que se apoyan.

Serie ISO/IEC 27.000

Las normas de la familia ISO 27.000, destacando fundamentalmente la ISO/IEC 27.001 e ISO/IEC 27.002, tienen como principales objetivos:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles proporcionales a los riesgos percibidos.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
- Generación y preservación de evidencias.
- Tratamiento de los incidentes de seguridad.
- Revisión y mejora continua del SGSI.
- Gestión de Riesgos
- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27.001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA).

Entre ellas existen normas que son básicamente una especificación de Requerimientos como la ISO/IEC 27.001 e ISO/IEC 27006. Otras son guías de implementación o lineamientos guía que son soporte del ciclo PHVA para los sistemas de gestión de la seguridad de la información, como la ISO/IEC 27003 o ISO/IEC 27.005.

A continuación, se describen brevemente los más relevantes para esta investigación:

“ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary”, provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI

“ISO/IEC 27001:2005 - Information technology - Security techniques - Information Security Management Systems - Requirements”, es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.

“ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management” - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos.

Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27.001.

“ISO/IEC 27003 - Information technology - Security techniques - Information security management system implementation guidance” - provee información práctica y una guía de implementación de la norma ISO/IEC 27001.

“ISO/IEC 27004 - Information technology - Security techniques - Information security management measurements” provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001.

“ISO/IEC 27005:2008 - Information technology - Security techniques - Information security risk management” – provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001.

“ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems” – establece los requerimientos para Organismos que prestan servicios de auditoría y certificación.

“ISO/IEC 27007 - Information technology - Security techniques - Information security management systems - Auditor guidelines” - provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.

2.3 NORMAS INTERNACIONALES RECONOCIDAS

2.3.1 COBIT. CObIT define una metodología y un marco de trabajo adecuado para la gestión de Tecnología de la Información (IT), orientado en el negocio y en procesos, y basado en controles. Para ello considera tres dimensiones: a) los dominios, procesos y actividades de IT; b) los requerimientos de la información del negocio; y c) los recursos de IT.

Define cuatro dominios, con sus procesos (34) que a su vez describen actividades concretas y especifican una serie de objetivos de control. Estos dominios son: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (ES), y Monitoreo y Evaluación (ME).

En particular, en el dominio PO, se centra la atención en la alineación de IT con los objetivos y estrategia del negocio, y en la gestión de riesgos. Así como en ES,

se especifica un proceso de “Aseguramiento de Continuidad del Servicio / Operaciones”.

A los efectos de satisfacer los objetivos de negocio se definen siete criterios en términos de requerimientos de la información, ellos son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento (marco legal y reglamentario, normas, contratos, etc.), y confiabilidad.

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

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la Información se define en el estándar como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran).

La ISO 27002 viene a ser un código en el que se recoge un catálogo de los controles de seguridad y una guía para la implantación de un SGSI. Está compuesta de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad. Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información. En la siguiente figura se muestra la distribución de dichos dominios y el aspecto de seguridad que cubren:

Figura 5. Estructura de ISO 27002

2.3.3 Norma OSSTMM. El Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet. Se encuentra en constante evolución y actualmente se compone de las siguientes fases:

Sección A -Seguridad de la Información

1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección B – Seguridad de los Procesos

1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección C – Seguridad en las tecnologías de Internet

1. Logística y Controles
2. Exploración de Red
3. Identificación de los Servicios del Sistema
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento

10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseñas
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

Sección D – Seguridad en las Comunicaciones

1. Testeo de PBX
2. Testeo del Correo de Voz
3. Revisión del FAX
4. Testeo del Modem

Sección E – Seguridad Inalámbrica

1. Verificación de Radiación Electromagnética (EMR)
2. Verificación de Redes Inalámbricas [802.11]
3. Verificación de Redes Bluetooth
4. Verificación de Dispositivos de Entrada Inalámbricos
5. Verificación de Dispositivos de Mano Inalámbricos
6. Verificación de Comunicaciones sin Cable
7. Verificación de Dispositivos de Vigilancia Inalámbricos
8. Verificación de Dispositivos de Transacción Inalámbricos
9. Verificación de RFID
10. Verificación de Sistemas Infrarrojos
11. Revisión de Privacidad

Sección F – Seguridad Física

1. Revisión de Perímetro
2. Revisión de monitoreo
3. Evaluación de Controles de Acceso
4. Revisión de Respuesta de Alarmas
5. Revisión de Ubicación
6. Revisión de Entorno

3. METODOLOGÍA

Esta investigación es de tipo Exploratoria con un enfoque Cualitativo, debido a que el objetivo que plantea es hacer un diagnóstico basado en la Norma ISO 27002.

La primera etapa de esta investigación será la recopilación y estudio de la Normas ISO 27001, ISO27002, COBIT, OSSTMM.

Seguida a la recolección de información vendrá una etapa de Análisis, se llevará a cabo una evaluación de herramientas disponibles actualmente en el mercado de SGSI y se obtendrá como resultado un análisis comparativo de éstas.

Una vez culminada la etapa de Análisis de Información se proseguirá a Diseñar y desarrollar un prototipo de una herramienta que apoye la gestión de controles de seguridad de la información, tomando como estándar ISO 27002.

Por último se darán a conocer los resultados del prototipo de software para el diagnóstico del estándar ISO 27002.

4. RESULTADOS

4.1 Cuadro Comparativo de los Estándares ISO 27001, ISO 27002, COBIT y OSSTMM

Tabla 3. Cuadro Comparativo de los Estándares ISO 27001, ISO 27002, COBIT y OSSTMM

CUADRO COMPARATIVO DE ESTÁNDARES				
CARACTERISTICA	**ISO 27001**	**ISO27002**	**COBIT**	**OSSTMM**
Ámbito	Seguridad de la Información	Seguridad de la Información	Gobierno de TI, que es el sistema por el cual se dirigen y controlan las TI en las Organizaciones	Metodología abierta de testeo de la Seguridad.
Orientación	Asegura la Selección de los Controles de Seguridad, adecuados y proporcionados para proteger la información	Es una guía para, en distintos ámbitos, conocer qué se puede hacer para mejorar la seguridad de la información	Gobierno de TI que indica las reglas y procedimientos para la toma de decisiones sobre las TI	Estándar de referencia. Test de seguridad en forma ordenada y con calidad profesional.
Tamaño	Consta de 39 objetivos de control y 133 controles	Consta de 11 dominios, 39 objetivos de control y 133 controles	Consta de 4 Dominios, 34 procesos de tecnologías de información y 318 objetivos de control.	Consta de 6 fases
Fortalezas	Diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a las partes interesadas	Manual de buenas prácticas y especificación de requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (mecanismos y controles).	Se aplica a los sistemas de información de cualquier empresa, en sistemas distribuidos, computadores personales y mini computadores	Es una guía que permite evaluar el nivel de seguridad de las tecnologías de información
Debilidades	Es necesario para su éxito el compromiso total de la Dirección y una definición clara del alcance.	Es necesario para su éxito el compromiso total de la Dirección y una definición clara del alcance.	Esta orientada al gobierno de TI, por esta razón no es fuerte en seguridad	Exige un alto nivel de especialización técnica y experiencia para los probadores que realizan las pruebas OSSTMM.

4.2 DISEÑO Y DESARROLLO DEL PROTOTIPO DE SOFTWARE

4.2.1 Metodología de desarrollo de software UML

4.2.1.1 Descripción del alcance y requerimientos. Se requiere el desarrollo e implementación de una herramienta de software que funcione en web que permita la gestión de cuestionarios, altamente configurables, como herramienta de auditoría para el diagnóstico del estándar ISO 27002 en cualquier organización. Para ello, se requiere que el sistema permita la gestión de cuestionarios, diferentes tipos de preguntas así como preguntas con diferentes opciones. De los ítems mencionados es importante almacenar id, título/nombre, descripción/enunciado, estado del registro y fecha y usuarios de última modificación. Así mismo, para poder calificar los cuestionarios es necesario que tanto las preguntas como sus opciones de respuesta (en caso de tenerlas) tengan la posibilidad de especificar un peso o valor porcentual. De acuerdo a lo anterior, se requiere almacenar también en el sistema los rangos de evaluación aplicables a cada cuestionario; esto es, de acuerdo a la puntuación obtenida en qué nivel, rango o escalafón se encuentra la organización y cuál es el diagnóstico que se hace.

Para gestionar la información de los cuestionarios se requiere de usuarios con diferentes perfiles que permitan separar la creación y modificación de la aplicación de cuestionarios. Es por esto que el sistema debe permitir también la gestión de usuarios y perfiles de usuario asociados a opciones de menú para poder otorgar o restringir el acceso a ciertas vistas de la aplicación.

Por otro lado, se requiere que el sistema permita almacenar la información de las veces que es utilizado o contestado un cuestionario, es decir, cada vez que se aplique para obtener un diagnóstico. Para ello se necesita que se almacene primero un encabezado que defina el cuestionario utilizado, la fecha, lugar y empresa en que se llevó a cabo, así como el usuario o auditor que lo aplica. Junto a este encabezado de cuestionario resuelto se almacenará el detalle del mismo, que comprende las respuestas dadas a cada pregunta del cuestionario seleccionado. De igual manera es pertinente tener registro de los resultados de cada evaluación y el nivel en que se encuentra respecto al estándar.

Adicional a lo anterior y para permitir la facilidad de implantación del sistema, se sugiere que cuente con una tabla de configuraciones que permita definir fácilmente temas como lenguaje, accesos FTP para un futuro manejo de archivos,

acceso a la base de datos, nombres y tags informativos del aplicativo, diseño general y plantillas, entre otros de interés.

REQUERIMIENTOS FUNCIONALES

- Permitir el registro de información sobre tipos de preguntas
- Permitir el registro de información sobre cuestionarios de auditoría a clientes
- Permitir el registro de información de preguntas de cuestionarios de auditoría a clientes
- Asignar preguntas al cuestionario que corresponda
- Permitir el registro de información de opciones de respuesta para preguntas
- Asignar opciones de respuesta a la pregunta que corresponda
- Permitir el registro de perfiles de usuarios
- Permitir el registro de usuarios del sistema
- Asignar perfiles de usuario a los usuarios registrados
- Permitir el registro de opciones de menú para definir las diferentes vistas del sistema.
- Asignar opciones de menú a perfiles de usuario para restringir o permitir el acceso a las diferentes vistas del sistema
- Permitir el registro de rangos de evaluación para los cuestionarios de consultoría a clientes.
- Asignar los rangos de evaluación pertinentes al cuestionario de consultoría a clientes. Estos rangos permitirán establecer los grados de madurez con que se califica a la empresa de acuerdo a las respuestas dadas al cuestionario.
- Registrar los intentos de respuesta de los cuestionarios de auditoría a clientes para permitir mantener un histórico de las aplicaciones de los mismos.

- Registrar las respuestas asociadas a cada intento/aplicación del cuestionario de auditoría a clientes.

- Evaluar la aplicación del cuestionario de clientes de acuerdo a los rangos de evaluación asignados y los pesos de las preguntas del cuestionario de acuerdo a las respuestas almacenadas.

- Mostrar al auditor el nivel en que se encuentra respecto al estándar la empresa evaluada.

- Registrar los resultados de la evaluación del cuestionario de auditoría a clientes.

REQUERIMIENTOS NO FUNCIONALES

- El sistema debe ser accesible desde cualquier navegador moderno de internet sin necesidad de instalar ningún complemento en el computador del cliente.

- El sistema no es accesible en todos los dispositivos móviles.

- El lenguaje de programación del lado del servidor será PHP.

- El servidor de gestión de base de datos será MySQL.

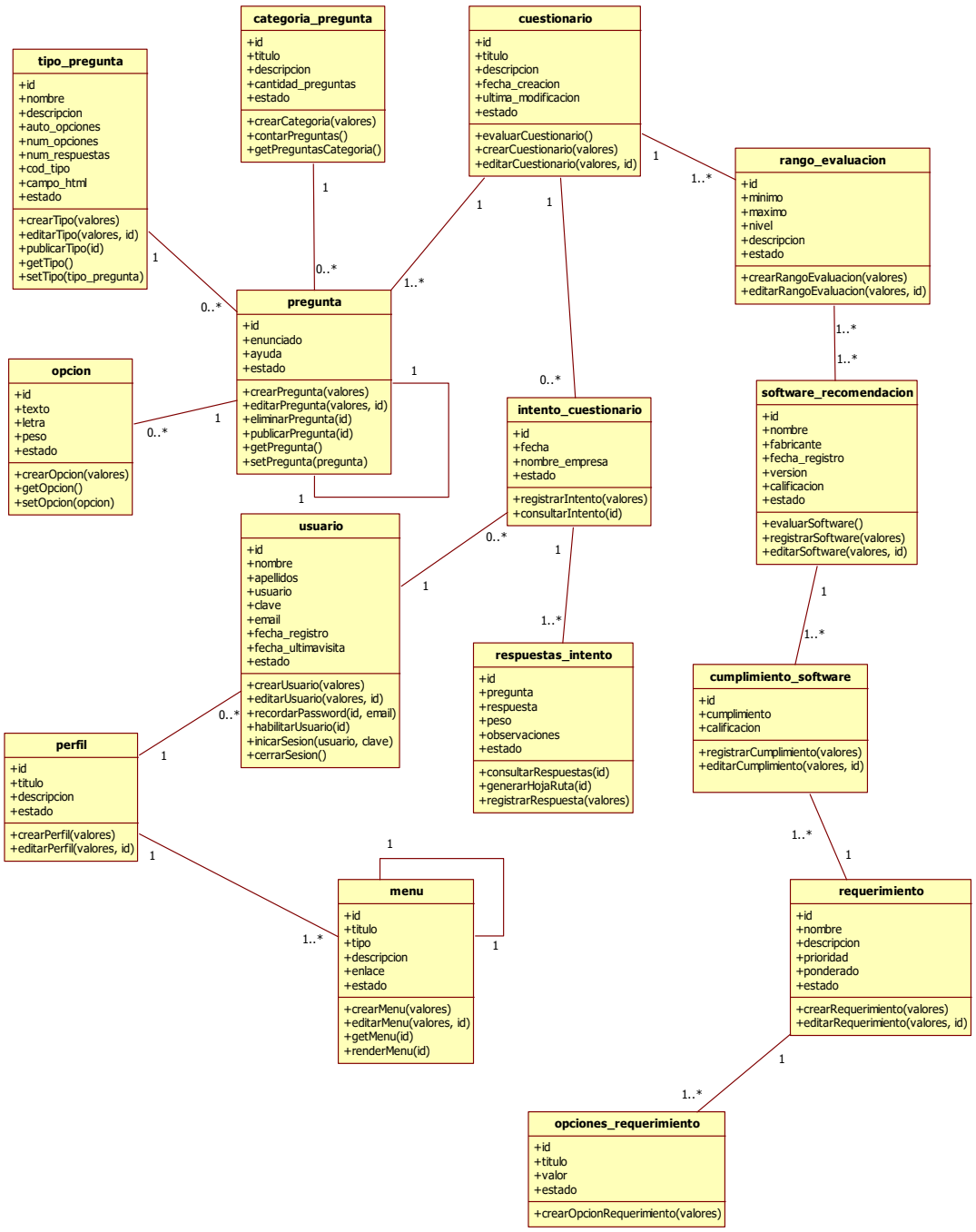
- Utilizar HTML y hojas de estilos CSS para el diseño de interfaz de usuario.

- Utilizar Javascript (del navegador) como lenguaje de programación del lado del cliente.

- Espacio mínimo de disco en el servidor de 500MB para el almacenamiento de archivos del sistema y base de datos.

4.2.1.2 Diagrama de Clases. Modelo de clases. Este modelo pretende ilustrar las relaciones entre las diferentes entidades/clases identificadas dentro del análisis del sistema de información para la aplicación de diagnóstico del estándar ISO 27002. De igual forma se describe a grandes rasgos los principales elementos de información (atributos de cada clase) y de funcionalidad (métodos de cada clase) del sistema. El sistema auditor tiene su centro en los cuestionarios y sus preguntas; así como en los rangos de evaluación que se asignen a los

cuestionarios y las herramientas de software que se registren en el sistema para servir como recomendación ante diferentes resultados obtenidos en el diagnóstico.



4.2.1.3 Diagrama de casos de uso

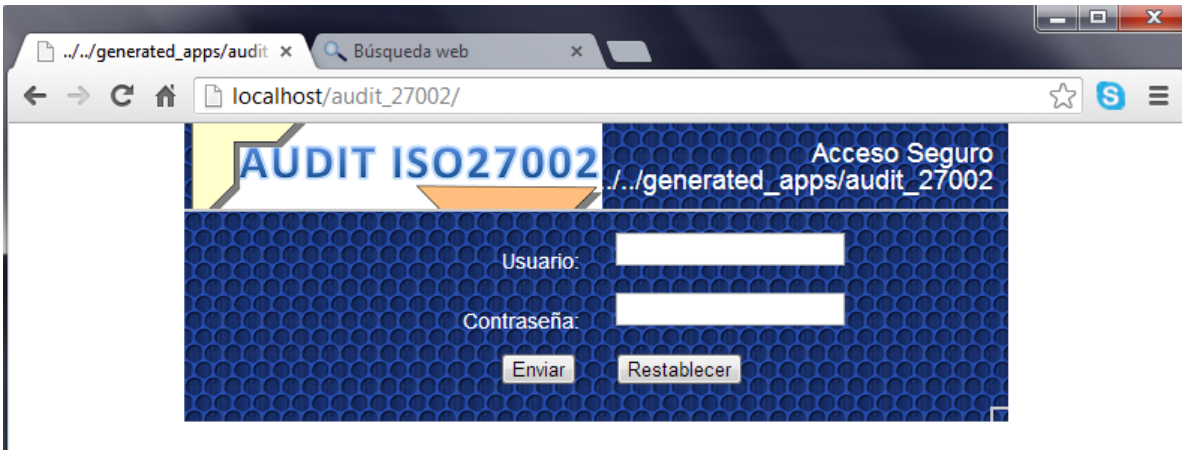
Diagrama de casos de uso. Expresa la funcionalidad del sistema en términos de los actores que interactúan con el mismo. El sistema de auditoría interactúa con dos actores: Auditores y Administradores. Los auditores se encargan de crear, editar y aplicar los cuestionarios de diagnóstico en las empresas. Además consultan los resultados de los diagnósticos.

Por otro lado, los administradores gestionan la configuración del sistema en términos de usuarios, perfiles de acceso, menús y parámetros de configuración adicionales (tales como conexión a base de datos, ftp, archivos, etc.).
El sistema, sin interacción directa con los actores, realiza la evaluación de los cuestionarios aplicados/diligenciados.

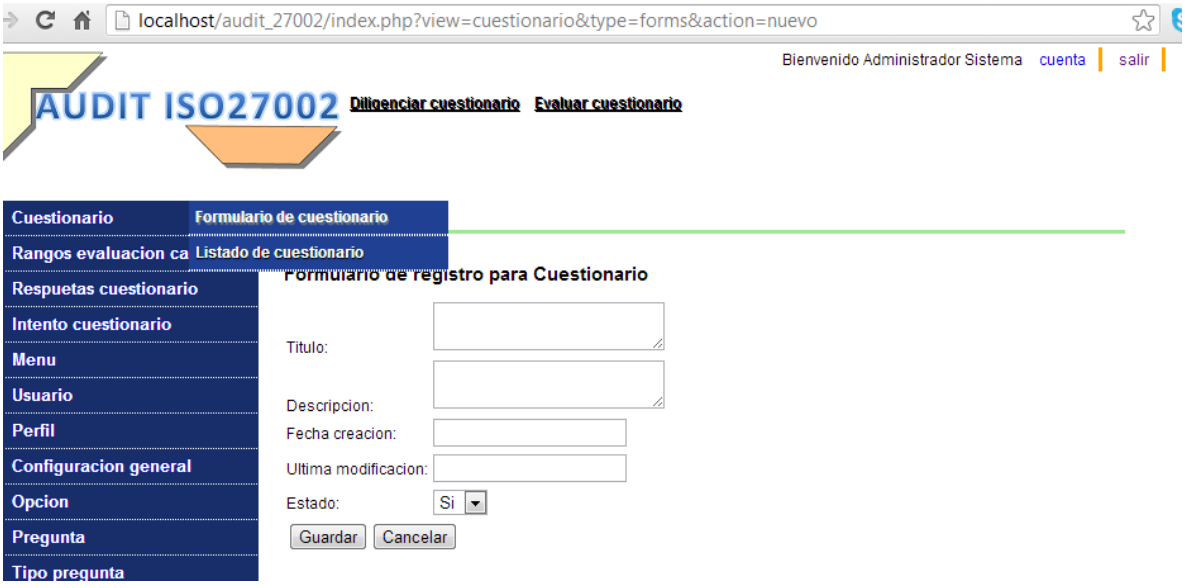
4.2.2 Resultados obtenidos con el prototipo de software. A través del sistema desarrollado se dispuso unas interfaces de captura de datos que permiten y obligan a seguir el proceso de metodológico de auditoría para el ingreso, procesamiento y generación de reportes. Encontrando los siguientes aspectos relevantes:

- El proceso de registro de la información es fácil e intuitivo y se valida automáticamente.

Login del usuario.



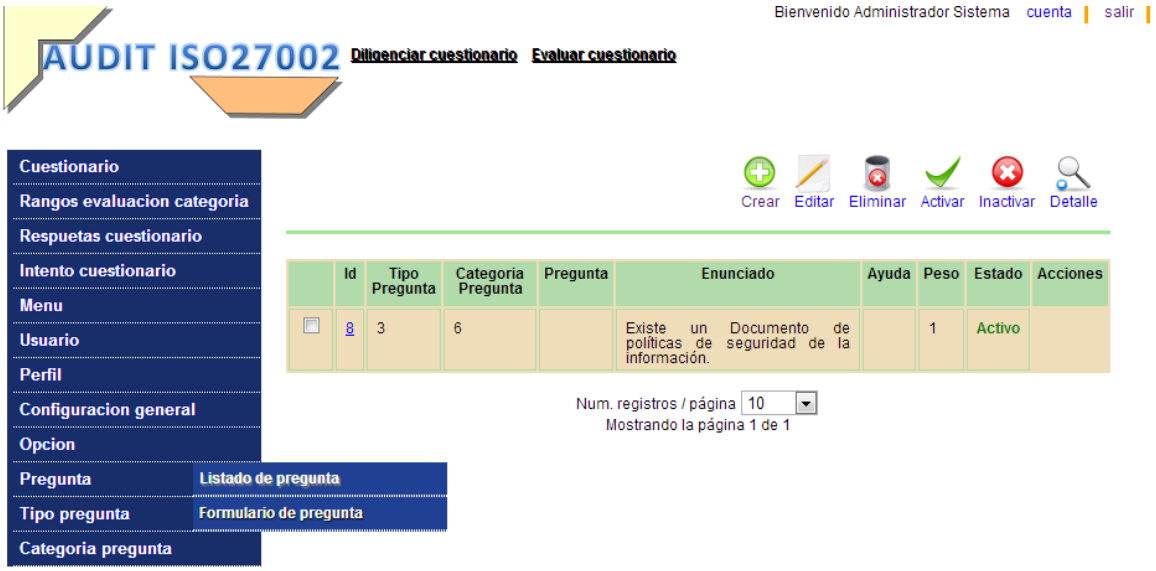
Creación del Cuestionario.



Listar Cuestionario.

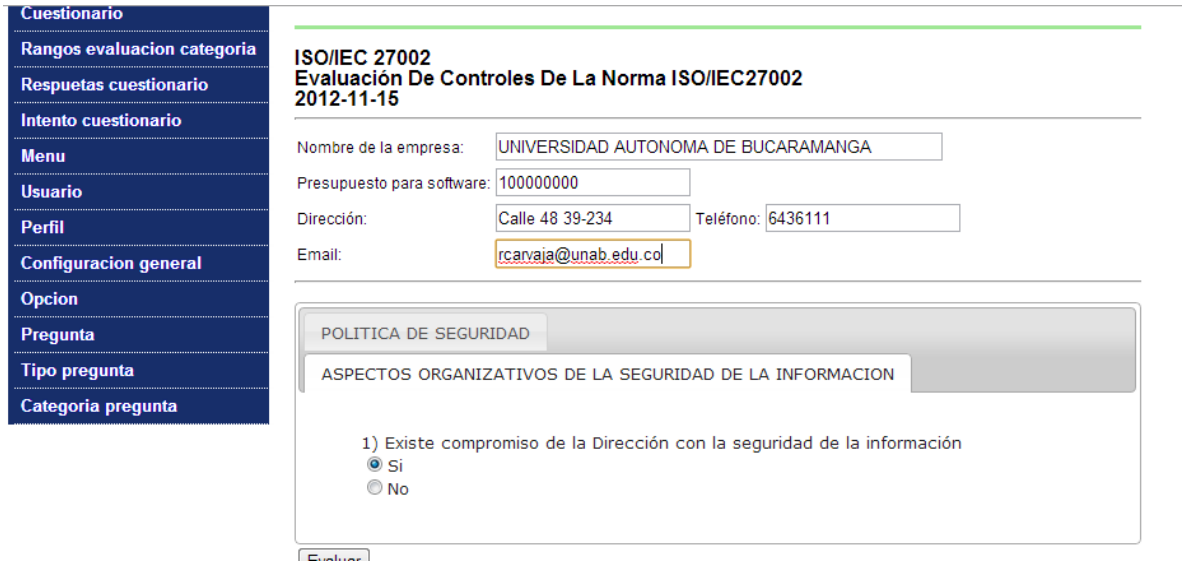
Categorías de las Preguntas

Preguntas



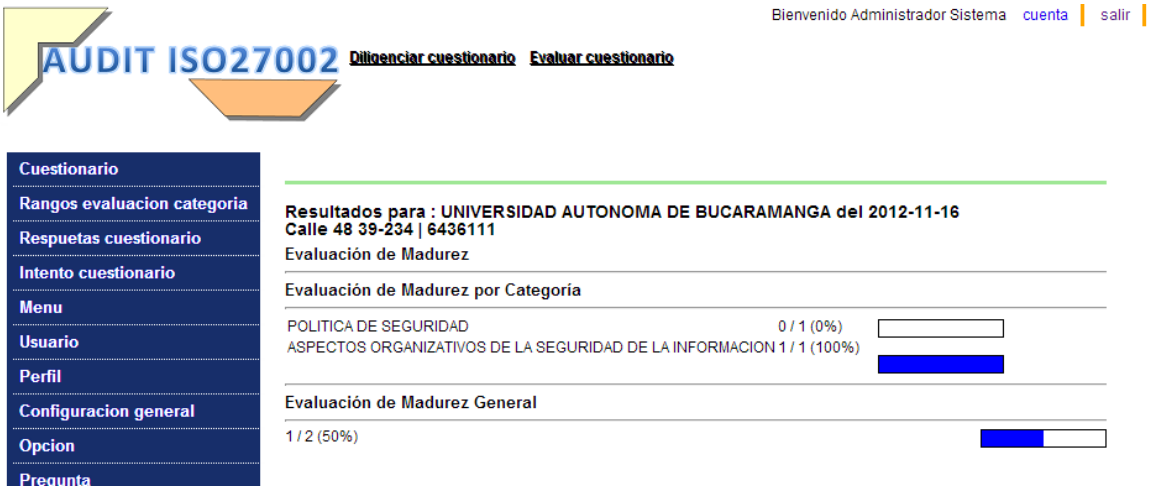
Diligenciar Cuestionario

Evaluar Cuestionario



Resultados Evaluación

4.



5. CONCLUSIONES

Se desarrolló un sistema web basado en software libre para el apoyo a la toma de decisiones sobre seguridad basado en el estándar internacional ISO 27002.

Por medio de los SGCSI se pueden abarcar lo referente al HPVA (Hacer, Planear, Verificar, Actuar), teniendo como base la norma ISO 27002 con sus respectivos dominios y controles; para su aplicación en las organizaciones y de ésta manera el equipo de seguridad soportar sus decisiones apoyado en los resultados obtenidos en la auditoria.

Por medio de este trabajo de grado se puede establecer que en el contexto general de las organizaciones el control de la gestión de seguridad de la información se encuentra aislada a la tomo de decisiones; permitiéndonos por medio de la herramienta generada un soporte sólido para establecer políticas claras y bien definidas, que apoye a las Directivas en su proceso de evaluación.

6. RECOMENDACIONES Y TRABAJOS FUTUROS

.

- El sistema generado permite la adaptación de otros estándares diferentes a la ISO 27002, tales como OSSTMM y COBIT

REFERENCIAS

Information Systems Audit and Control Association. ISACA, Disponible en Internet: http://www.isaca.org/

IT Infrastructure Library, ITIL. IT Service Management (ITSM), Office of Government Commerce. (OGC), UK. Disponible en Internet: http://www.itil-itsm-world.com/ (octubre de 2009).

ISO/IEC 27000 “Information technology - Security techniques - Information security management. systems - Overview and vocabulary”

International Organization for Standarization (ISO), Disponible en Internet: http://www.iso.org/

ROSS R., Katzke S., Johnson A., Swanson M., Stoneburner G., “Managing Risk from Information
Systems - An Organizational Perspective (second public draft)”, NIST SP 800-39, National
Institute of Standards and Technology, U.S. Department of Commerce
http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf (octubre de 2009).

IQBAL, A.; Horie, D.; Goto, Y.; Jingde Cheng. (2009). A Database System for Effective Utilization of ISO/IEC 27002. In Proceedings of the 2009 Fourth International Conference on Frontier of Computer Science and Technology (FCST '09). IEEE Computer Society, Washington, DC, USA, 607-612. Recuperado el 8 de octubre de 2011 de la base de datos IEEE Xplore Digital Library.

HORVÁTH, M.; Jakub, M. (2009). Implementation of security controls according to ISO/IEC 27002 in a small organization. Quality Innovation Prosperity, 13 (2), 48-54. Recuperado el 10 de octubre de 2011 de DOAJ - Directory of Open Access Journals. Disponible en Internet: http://www.qip-journal.eu/files/2009/2009-2/QIP_2_2009_Horvath.pdf

GERBER, M.; Vonsolms, R. (2008). Information security requirements – Interpreting the legal aspects. Computers Security, 27 (5-6), 124-135. Elsevier Ltd. Recuperado el 10 de octubre de 2011 de la base de datos ScienceDirect.

Disponible en Internet: http://linkinghub.elsevier.com/retrieve/pii/S0167404808000461

BYLICA, W.; Ksiezopolski, B. (2011). On Scalable Security Audit for Web Application According to ISO 27002. Computer Networks, 160, 289-297. Recuperado el 10 de octubre de 2011 de Springer Berlin Heidelberg. Disponible en Internet: http://dx.doi.org/10.1007/978-3-642-21771-5_31

KNAPP, K. J., Franklin Morris Jr., R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers Security, 28(7), 493-508. Elsevier Ltd. Disponible en Internet: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000765

KLAIC, A. Hadjina, N. (2011). Methods and tools for the development of information security policy — A comparative literature review. MIPRO, 2011 Proceedings of the 34th International Convention , vol., no., pp.1532-1537, 23-27 May 2011. Disponible en Internet: http://www.sinab.unal.edu.co:2365/stamp/stamp.jsp?tp=&arnumber=5967304&isnumber=5967009

CALDER, A. (2009). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing.

Icontec. (2009). Compendio: sistema de gestión de la seguridad de la información (SGSI). Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC.

Alexander, A. (2007). Diseño de un sistema de gestión de seguridad de información: óptica ISO 27001:2005. Alfaomega Colombiana.