SOFTWARE PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL BASADO EN LA NORMA ISO/IEC 27001 DE 2013

Ing. José Daniel Guerra Eraso

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Programa de Especialización en Seguridad Informática
Pasto, noviembre de 2015

SOFTWARE PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL BASADO EN LA NORMA ISO/IEC 27001 DE 2013

ING. JOSÉ DANIEL GUERRA ERASO

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Programa de Especialización en Seguridad Informática
Pasto, noviembre de 2015

SOFTWARE PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL BASADO EN LA NORMA ISO/IEC 27001 DE 2013

Ing. José Daniel Guerra Eraso

Trabajo de grado presentado como requisito para optar al título de
Especialista en seguridad informática

Líder nacional del programa:

Esp. RAMSES RÍOS LAMPRELLO
Ingeniero de sistemas, líder nacional del programa ESI

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Programa de Especialización en Seguridad Informática
Pasto, noviembre de 2015

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

JURADO CALIFICADOR

_____

JURADO CALIFICADOR

SAN JUAN DE PASTO, JUNIO DE 2016

AGRADECIMIENTOS

El desarrollo de este proyecto ha sido un largo camino lleno de dificultades y sacrificios desde el inicio de la especialización hasta la entrega final. Esas piedras en el camino han demorado la entrega y obtención de resultados pero gracias al esfuerzo propio y al de otras personas finalmente puedo presentar este proyecto. Agradezco infinitamente a mi esposa quien con su paciencia, su optimismo y su cariño me ha dado ánimos de continuar y terminar cada proyecto, agradezco al cuerpo docente de la Especialización en seguridad informática de la UNAD por regalarme momentos tan agradables, apoyo y guía pero sobre todo por proponer retos que, al superarlos pude darme cuenta de cuan capaz puedo llegar a ser, agradezco en especial a mi asesor en el desarrollo del proyecto, el docente FRANCISCO SOLARTE, cuyos consejos e interés en el tema que se aborda en este documento ha sido de enorme ayuda y su respaldo ha sido clave desde mi pregrado.

CONTENIDO

RESUMEN 13
INTRODUCCIÓN 14
1. CAPITULO 1: PROBLEMA 16
1.1. DESCRIPCIÓN DEL PROBLEMA 16
2. CAPITULO 2: OBJETIVOS DEL PROYECTO 17
2.1. OBJETIVO GENERAL 17
2.2. OBJETIVOS ESPECÍFICOS 17
3. CAPITULO 3: MARCO REFERENCIAL 18
3.1. ANTECEDENTES: 18
3.2. MARCO TEÓRICO 19
3.2.1. Ingeniería del software 19
3.2.2. Análisis y diseño de sistemas 20
3.2.3. Proceso de Software 21
3.2.4. Modelo de proceso de software 22
3.2.5. Paradigmas del desarrollo 23
3.2.6. Modelos ágiles de desarrollo de software 24
3.2.7. Modelo de prototipos 26
3.2.8. UML - Lenguaje Unificado de Modelado 28
3.2.9. Aplicaciones web y aplicaciones de escritorio 29
3.2.10. Lenguaje de programación PHP 31
3.2.11. DBMS (en español SGBD - Sistema de Gestión de Base de Datos) 33
3.2.12. MySQL 34
3.2.13. Bases de datos 35
3.2.14. Diseño de una base de datos 35
3.2.15. Modelo relacional 36
3.2.16. SQL (Structured Query Language) 37
3.2.17. La serie ISO 27000 37
3.2.18. ISO/IEC 27001 40

3.2.19. Objetivos Controles de la norma ISO 27001 (V. 2013) 41
3.2.19.1. Modelo de procesos "*Planear-Hacer-Verificar-Actuar*" 44
3.2.20. ISO/IEC 27002 46
3.2.21. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 55
3.2.22. ESTABLECIMIENTO Y GESTIÓN DEL SGSI 56
3.2.23. IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI 57
3.2.24. SEGUIMIENTO Y REVISIÓN DEL SGSI 57
3.2.25. MANTENIMIENTO Y MEJORA DEL SGSI 59
3.3. MARCO CONCEPTUAL 60
3.3.1. Seguridad de la información 60
3.3.2. Integridad 60
3.3.3. Disponibilidad 60
3.3.4. Confidencialidad 61
3.3.5. Riesgo-Vulnerabilidad-Amenaza 61
3.3.5.1. Riesgo 61
3.3.5.2. Amenaza 62
3.3.5.3. Vulnerabilidad 62
3.3.6. Control informático 63
3.3.7. Modelo de madurez 64
3.3.8. Tipos de Controles 65
3.3.8.1. Controles Preventivos 65
3.3.8.2. Controles Detectivos 65
3.3.8.3. Controles Correctivos 65
3.3.9. Software 66
3.3.10. Proceso de software 67
3.3.11. Requerimientos 67
3.3.12. Prototipo de software 69
3.4. MARCO LEGAL 70
4. CAPITULO 4: DISEÑO METODOLÓGICO 78
4.1. FASES DE DESARROLLO 78

4.1.1. Fase 1: Recolección de información. 78
4.1.2. Fase 2: Análisis. 78
4.1.3. Fase 3: Diseño y desarrollo. 78
4.1.4. Fase 4: Validación y pruebas. 78
4.1.5. Fase 5: Documentación y recomendaciones. 79
4.2. DESCRIPCIÓN GENERAL DE ACTIVIDADES 79
4.3. METODOLOGÍA DE LA INVESTIGACIÓN 81
4.3.1. MODELO DE DESARROLLO 81
5. CAPÍTULO 5: EJECUCIÓN DEL PROYECTO 82
5.1. ANTECEDENTES ISO 27001:2005 - ISO 27001:2013 82
5.1.1. ESTRUCTURA DE LA NUEVA VERSIÓN ISO 27001:2013 82
5.1.2. PROPUESTA ACTUALIZADA DE LOS OBJETIVOS DE CONTROL 83
5.1.3. EVALUACIÓN DE CONTROLES Y ESTADISTICAS 86
5.1.3.1. NIVEL DE MADUREZ EN LA SEGURIDAD DE LA INFORMACIÓN 86
5.1.3.2. CARACTERISTICAS DE LA CALIDAD DE LA INFORMACIÓN 87
5.2. DISEÑO DEL SOFTWARE 89
5.2.1. INGENIERIA DE REQUERIMIENTOS 89
5.2.1.1. Identificación de actores 89
5.2.1.2. Requerimientos funcionales 90
5.2.1.3. Requerimientos no funcionales 91
5.2.2. DISEÑO ORIENTADO A OBJETOS 92
5.2.2.1. Diagramas de casos de uso 92
5.2.2.2. Diagramas de secuencia 97
5.2.3. MAPA FUNCIONAL DEL SOFTWARE 99
5.2.4. DISEÑO DE LA INTERFAZ DE USUARIO 100
5.2.5. DISEÑO DE BASE DE DATOS 105
6. CAPITULO 6: DESARROLLO 108
6.1. MÓDULO PROYECTO 108
6.2. MÓDULO ESTADISTICAS 109
6.3. MODULO CUESTIONARIOS 109

6.4. MODULO REPORTES 110

6.5. BOTON AYUDA 111

7. CAPITULO 7: VALIDACIÓN Y PRUEBAS 112

7.1. ORGANIZACIÓN 1: Fundación de servicios educativos de EMSSANAR - CETEM 112

7.2. ORGANIZACIÓN 1: INSTITUCIÓN UNIVERSITARIA CESMAG. (Facultad Ingeniería) 113

7.3. ORGANIZACIÓN 1: EPS Indígena MALLAMAS 113

8. CAPITULO 8: DISCUSIÓN Y ANÁLISIS DE RESULTADOS 115

9. REFERENCIAS 120

LISTA DE ILUSTRACIONES

Ilustración 1: Modelo prototipos 26
Ilustración 3: Conceptos básicos modelo relacional 36
Ilustración 4: Modelo PHVA aplicado a los procesos de SGSI 45
Ilustración 5: estructura ISO 27001:2013 83
Ilustración 6: Anexo "A" ISO 27001: 2013 84
Ilustración 7: Modelo Prototipo Incremental del proyecto 81
Ilustración 8: Mapa funcional del software 99

LISTA DE TABLAS

Tabla 1: Comparativa DBMS 33
Tabla 2: Descripción del modelo PHVA 45
Tabla 3: Dominios, objetivos de control y controles ISO/IEC 27002..... 46
Tabla 4: Descripción general de actividades del presente proyecto 79
Tabla 5: Cambios de controles ISO 27001..... 85
Tabla 6: Actores del proyecto 90

ANEXOS

ANEXO 1 - Manual de usuario del software

ANEXO 2 - ISO27k Controls cross check

ANEXO 3 - Formato encuesta funcionamiento del software

ANEXO 4 – Reporte general CETEM

ANEXO 5 – Reporte general IU CESMAG

ANEXO 6 – Reporte general EPSI MALLAMAS

ANEXO 7 – Enlace de acceso EVA27

RESUMEN

Este trabajo de posgrado propone un método de diagnóstico del estado de la seguridad informática empresarial a través del estado de los controles de su sistema de gestión de seguridad de la información SGSI según la norma ISO/IEC 27001 de 2013 analizándolos con el uso de una solución de software que pretende dinamizar y facilitar este proceso además de permitir su gestión sobre diferentes tipos de organizaciones. La presente propuesta no pretende entrar en conflicto con esta clase de proyectos sino más bien simplificar la obtención de resultados e incluso anexarse como herramienta de apoyo que facilite, dinamice y promueva la implantación y mejora de un SGSI.

PALABRAS CLAVE

Diagnóstico, Auditoría, Controles, Seguridad de la información, riesgos.

INTRODUCCIÓN

Hace algún tiempo se hablaba de los grandes cambios y de la incidencia de la era de la información, de cómo la humanidad se hacía cada vez más dependiente de los sistemas informáticos, ya no solo a nivel laboral o empresarial sino en todos los ambientes. Es innegable que dicho panorama ya no es más una visión futurista sino que describe el escenario actual.

La información se convierte ahora en el activo vital que permite a una organización garantizar su continuidad y, debido a que todo gira alrededor de la información, la competitividad solo puede ser un sinónimo de calidad de la información (disponibilidad, integridad y confidencialidad).

Teniendo en cuanta lo mencionado anteriormente, se hace ineludible que todas las empresas inicien el proceso de diagnóstico actual de la seguridad de la información y de las aplicaciones informáticas que en su gran mayoría funcionan sobre sistemas de red o son aplicaciones web.

Para solucionar este inconveniente se hace necesaria la creación de una herramienta que permita hacer un diagnóstico de manera ágil y sin incurrir en los altos costos que implicaría una auditoría a la seguridad de la información dentro de una organización. El software debe permitir que el proceso de evaluación pueda ser realizado para organizaciones de distinto tipo de actividad económica y para organizaciones de todos los tamaños.

La herramienta de software debe permitir la evaluación de todos los dominios de la norma ISO/IEC 27001 de 2013 que son 14, y en cada uno de ellos determinar el nivel de cumplimiento, a través de la aplicación de listas de chequeo que serán diseñadas para su medición.

El software contará con una interfaz de fácil manejo, una base de datos que puede ser alimentada con los cuestionarios diseñados de acuerdo a la norma y con un sistema de reportes textuales para identificar que controles (políticas y procedimientos) que haga falta definir, así como reportes gráficos que muestren el estado actual frente a las respuestas de cada uno de los checklist aplicados.

Con esos reportes generados dinámicamente, los ingenieros de sistemas encargados del área informática pueden establecer los planes de mejoramiento de la seguridad de la información frente a posibles ataques que puedan suceder al

futuro, estableciendo Sistemas de Gestión de Seguridad de la Información (SGSI) adecuados para cada organización.

Se eligió la norma ISO/IEC 27001 por ser una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector público o privado o de cualquier parte del mundo, esta norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad, sector público y tecnología de la información (TI). Además esta norma, es la única norma internacional auditable que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), ya que está concebida para garantizar la selección de controles de seguridad adecuados y proporcionales.

Así como la norma ISO 27001 promueve la calidad de la información, una aplicación dinámica de la misma a través de una herramienta de software potencia, agiliza y facilita su implementación trayendo consigo todas las ventajas de la norma a organizaciones con cualquier nivel de experiencia en auditoría informática.

1. CAPITULO 1: PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

Los recursos informáticos de una empresa son una constante ya que permiten agilizar los procesos de información. Junto con los avances informáticos surgieron nuevas formas de ataques que hacen vulnerables los sistemas de cualquier organización y por esta razón emergen también métodos de protección que están en continua evolución, primero como un conjunto de prácticas y más tarde como estándares aceptados a nivel internacional, diseñados para que ser aplicados y que tienen como objetivo la certificación que garantiza al consumidor la seguridad de la información de los trámites y servicios prestados por la empresa en cuanto a la disponibilidad, integridad y confidencialidad de la información.

El problema que se presenta es la casi nula existencia de herramientas de software que permitan determinar el cumplimiento de los estándares de seguridad actuales para lograr establecer un sistema de gestión de seguridad adecuado y que ayuden a alcanzar la certificación de la seguridad de la información, se ha verificado la existencia de software para realizar procesos de análisis y evaluación de riesgos que permiten determinar el nivel de exposición y el impacto, pero no hay herramientas de libre uso que permitan hacer el diagnóstico y evaluación de la seguridad sin incurrir en los altos costos que ello implica.

Una de las razones más importantes que se puede identificar del porqué de esta situación es que si una empresa no conoce su estado actual de seguridad (o inseguridad) respecto a un determinado estándar, tampoco va a dar mucha importancia a los cambios que pueda necesitar para mejorar y quizá ni siquiera pueda observar necesidad alguna.

Cada vez es más importante determinar el estado actual de las organizaciones frente a la seguridad de la información, por esta razón se hace indispensable que se elabore una herramienta que permita la evaluación haciendo uso de un producto de software sin incurrir en los altos costos que implica realizar procesos de auditoría y por los cuales las empresas quieren seguir como están y no desean este tipo de diagnósticos.

2. CAPITULO 2: OBJETIVOS DEL PROYECTO

2.1. OBJETIVO GENERAL

Desarrollar una solución de software basado en la norma ISO/IEC 27001 del 2013 que permita evaluar y determinar el estado del sistema de gestión de seguridad de la información (SGSI) y su evolución en cualquier organización que busque certificarse bajo dicha norma o que sencillamente desee mejorar su nivel de seguridad informática.

2.2. OBJETIVOS ESPECÍFICOS

- Hacer un estudio sobre la norma ISO/IEC 27001 de 2013, para determinar los cambios en la misma con respecto a la versión de 2005, y determinar antecedentes relacionados con el tema.

- Definir y analizar los requerimientos del software a desarrollar, determinando las funcionalidades, la base de datos y los reportes necesarios que deberán implementarse

- Diseñar el software para ser desarrollado en lenguajes orientados a la web que de acuerdo a la información recolectada y las características definidas permitan realizar un diagnóstico con base en la norma mencionada y generar informes de fácil interpretación.

- Implementar el software y realizar pruebas de validación de cada módulo y funcionalidad independiente del software según el modelo de desarrollo que sea más adecuado para este fin.

- Determinar si los resultados del diagnóstico son fiables a través de su aplicación en una organización real mirando los resultados a través de los reportes generados por el software y la utilidad de los mismos para los auditores de seguridad.

3. CAPITULO 3: MARCO REFERENCIAL

3.1. ANTECEDENTES:

- ***Seguridad Global de su Información "Global SGSI", AUDISEC***

  Es una herramienta software que ha sido lanzada al mercado por la empresa española de seguridad en la información *AUDISEC*, en el mes de septiembre de 2008.

  Esta herramienta se desarrolló para la gestión integral de la norma ISO 27001:2005 en las empresas españolas, según información del Director de ISO 27001 de AUDISEC España, Alejandro Delgado Gallego.

- *"ERAZO ARCINIEGAS Andrea, MORAN BRAVO Carmen, Políticas de seguridad para el área de sistemas del instituto Colombiano de bienestar familiar regional Nariño, San Juan de Pasto, Proyecto de grado, IU CESMAG"*

  En este estudio, basado en el Instituto Colombiano de Bienestar Familiar se demostró la existencia de algunas deficiencias en el manejo de los recursos informáticos y en especial deficiencias en la seguridad de acceso físico a las instalaciones del área de sistemas y acceso lógico a la información.

  Es relevante porque determina las políticas de seguridad informática de una institución pública frente a un conjunto de deficiencias y que pueden ser comunes y que están contenidas en la norma ISO/IEC 27001 como el acceso a recursos físicos, lógicos y a la información.

- *"PATIÑO ALPALA Luis Olmedo, Propuesta De Actualización, Apropiación Y Aplicación De Políticas De Seguridad Informática En Una Empresa Corporativa, Propolsinecor, San Juan de Pasto, Proyecto de grado, UNAD"*

  En este proceso de investigación, basado en Propolsenicor, se pudo establecer que hace falta una estructura jerárquica dedicada exclusivamente al manejo de la seguridad de la información, como también herramientas que permitan monitorear la red y probar la vulnerabilidad de los aplicativos.

  Por otra parte se estableció que la compañía tiene un sistema de seguridad informática que contempla algunos apartes de la norma estándar ISO NTC 27001, implementada como controles de seguridad de la información en los procesos de calidad de la ISO NTC 9001, con unas

políticas de seguridad informática llamados controles, encontrándose debilidades en cuando a la poca difusión y capacitación en la implementación del sistema de seguridad informática.

3.2. MARCO TEÓRICO

3.2.1. Ingeniería del software[1]

Es la disciplina o área de la informática que ofrece métodos y técnicas para desarrollar y mantener software de calidad.

Esta ingeniería trata con áreas muy diversas de la informática y de las Ciencias de la Computación, tales como construcción de compiladores, Sistemas Operativos, o desarrollos Intranet/Internet, abordando todas las fases del ciclo de vida del desarrollo de cualquier tipo de Sistema de Información y aplicables a infinidad de áreas (negocios, investigación científica, medicina, producción, logística, banca, control de tráfico, meteorología, derecho, Internet Intranet, etc.).

La ingeniería del software es el establecimiento y uso de principios robustos de la ingeniería a fin de obtener económicamente software que sea fiable y que funcione eficientemente sobre maquinas reales

Los fundamentos de la ingeniería del software es la capa del proceso. El proceso de la ingeniería del software es la unión que mantiene juntas las capas de tecnología y que permite un desarrollo racional y oportuno de la ingeniería del software. El proceso define un marco de trabajo para un conjunto de aéreas clave de proceso, que se deben establecer para la entrega efectiva de la tecnología de la ingeniería del software. Las aéreas claves del proceso forman la base del control de gestión de proyectos del software y establecen el contexto en el que se aplican los métodos técnicos, se obtienen productos del trabajo (modelos, documentos, datos, informes, formularios, etc), se establecen hitos, se asegura la calidad y el cabio de gestión adecuadamente.

Los métodos de la ingeniería del software indican cómo construir técnicamente el software. Los métodos abarcan una gran gama de tareas que incluyen análisis de requisitos, diseño, construcción de programas, pruebas y mantenimiento. Los métodos de la ingeniería del software dependen de un conjunto de principios básicos que

[1]Tomado de: INGENIERÍA DE SOFTWARE: UN ENFOQUE PRÁCTICO - Pressman, Roger S. - 5 ª Edición

gobiernan cada área de la tecnología e incluyen actividades de modelado y otras técnicas descriptivas.

Las herramientas de la ingeniería del software proporcionan un enfoque automático o semiautomático para mientras para el proceso y para los métodos. Cuando se integran herramientas para que la información creada por una herramienta la pueda utilizar otra, se establece un sistema de soporte para el desarrollo del software llamado ingeniería del software asistida por computadoras.

La ingeniería del software es una tecnología multicapa que debe apoyarse sobre un compromiso de organización de calidad, es por esto que realiza análisis, diseño, construcción, verificación y gestión de entidades técnicas o sociales. Con independencia de la entidad a la que se va a aplicar ingeniería, se debe cuestionar y responder las siguientes preguntas:

- Cuál es el problema a resolver?
- Cuáles son las características de la entidad que se utiliza para resolver el problema?
- Como se realizara la entidad (y solución)?
- Como se construirá la entidad?
- Que enfoque se va a utilizar para no complementar los errores que se cometieron en el diseño y en la construcción de la entidad?
- Como se apoyara la entidad cuando usuarios soliciten correcciones, adaptaciones y mejoras de la entidad?

3.2.2. Análisis y diseño de sistemas[2]

Los sistemas de información se desarrollan con diferentes propósitos, los cuales dependen de las necesidades de las empresas. Los sistemas de procesamiento de datos, los sistemas de información para la administración (MIS, Management Information System), y los sistemas de apoyo para la toma de decisiones (DSS, Decision Support System), diferentes tipos de sistemas de información computarizados que se analizan y diseñan mediante la aplicación de los conceptos y las técnicas del diseño y del análisis del sistema. En cierto grado, esto también se aplica a los sistemas expertos.

- Sistemas de procesamiento de datos

[2]ANÁLISIS Y DISEÑO DE SISTEMAS - Kendall, Kenneth E. y Kendall, Julie, E. - 3ª. Edición

- Sistemas informáticos para la administración
- Sistemas expertos e inteligencia artificial
- Sistemas de apoyo para la toma de decisiones: Es un tipo de sistema de información computarizada (DSS: Decision Support System). El sistema de apoyo para la toma de decisiones es similar a los sistemas de información tradicionales para la administración, en el sentido de que ambos dependen de una base de datos como fuente de información: pero se distingue del sistema de información para la administración, al hacer énfasis en el soporte en cada una de las etapas de la toma de decisiones se diseñan con una orientación hacia la persona o el grupo que los utilizara, y no como los sistemas de información tradicionales para la administración.

El análisis y el diseño de sistemas, tal como lo realizan los analistas de sistemas, pretenden estudiar sistemáticamente la operación de ingresos de los datos, el flujo de los mismos y la salida de la información: todo ello del contexto de una empresa en particular. En suma, el análisis y diseño de sistemas sirve para analizar, diseñar y fomentar mejoras en la operación de la empresa, lo cual puede realizarse mediante el uso de sistemas de información computarizados.

Si un sistema se instala sin una planeación adecuada, es muy probable que no sea satisfactorio y después, quede en el olvido. El análisis y diseño de sistemas permite estructurar el costoso esfuerzo de la implementación de los sistemas de información, que de otra manera ocurrirá de manera azarosa. El diseño y análisis de sistemas se conforman por una serie de procesos, que al ejecutarse sistemáticamente mejoran la operación de un negocio, mediante el uso de los sistemas de información computarizados. Una buena parte del análisis y el diseño de sistemas involucran el trabajo en colaboración con los usuarios actuales de tales sistemas de información.

3.2.3. Proceso de Software[3]

Un proceso del software es un conjunto de actividades y resultados asociados que producen un pro-duelo de software. Estas actividades son llevadas a cabo por los ingenieros de software.
Existen cuatro actividades fundamentales de procesos (que iremos estudiando progresivamente en el transcurso del módulo) que son comunes para todos los procesos del software. Estas actividades son:

[3]ANÁLISIS Y DISEÑO DE SISTEMAS - Kendall, Kenneth E. y Kendall, Julie, E. - 3ª. Edición

- **Especificación** del software donde los clientes e ingenieros definen el software a producir y las restricciones sobre su operación. (comunicación)
- **Desarrollo** del software donde el software se diseña y programa.
- **Validación** del software donde el software se valida para asegurar que cumple con los requerimientos del cliente.
- **Evolución** del software donde el software se modifica para adaptarlo a los cambios requeridos por el cliente y el mercado.

Diferentes tipos de sistemas necesitan diferentes procesos de desarrollo. Por ejemplo, el software de tiempo real en un avión tiene que ser completamente especificado antes de que empiece el desarrollo, mientras que en un sistema de comercio electrónico, la especificación y el programa normalmente son desarrollados juntos. Por lo tanto, estas actividades genéricas pueden organizarse de diferentes formas y describirse en diferentes niveles de detalle para diferentes tipos de software. Sin embargo, el uso de un proceso inadecuado del software puede reducir la calidad o la utilidad del producto de software que se va a desarrollar y/o incrementar los costes de desarrollo.

3.2.4. Modelo de proceso de software[4]

Un modelo de procesos del software es una descripción simplificada de un proceso del software que presenta una visión de ese proceso. Estos modelos pueden incluir actividades que son parte de los procesos y productos de software y el papel de las personas involucradas en la ingeniería del software. Algunos ejemplos de estos tipos de modelos que se pueden producir son:

- **Un modelo de flujo de trabajo.** Muestra la secuencia de actividades en el proceso junto con sus entradas, salidas y dependencias. Las actividades en este modelo representan acciones humanas.
- **Un modelo de flujo de datos o de actividad**. Representa el proceso como un conjunto de actividades, cada una de las cuales realiza alguna transformación en los datos.
  Muestra cómo la entrada en el proceso, tal como una especificación, se transforma en una salida, tal como un diseño. Pueden representar transformaciones llevadas a cabo por las personas o por las computadoras.

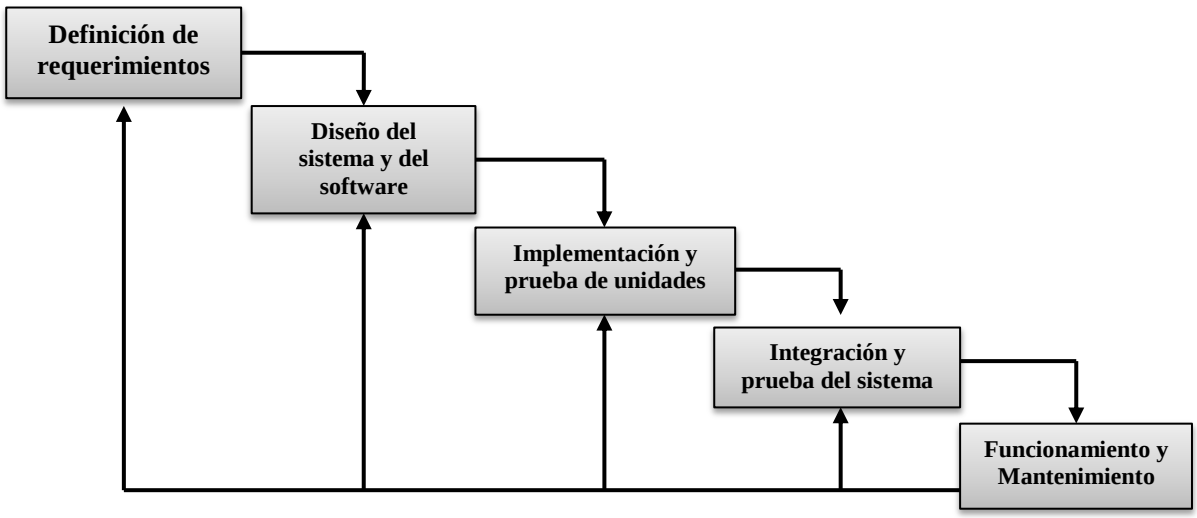
[4]ANÁLISIS Y DISEÑO DE SISTEMAS - Kendall, Kenneth E. y Kendall, Julie, E. - 3ª. Edición

Un modelo de rol/acción. Representa los roles de las personas involucrada en el proceso del software y las actividades de las que son responsables.

3.2.5. Paradigmas del desarrollo[5]

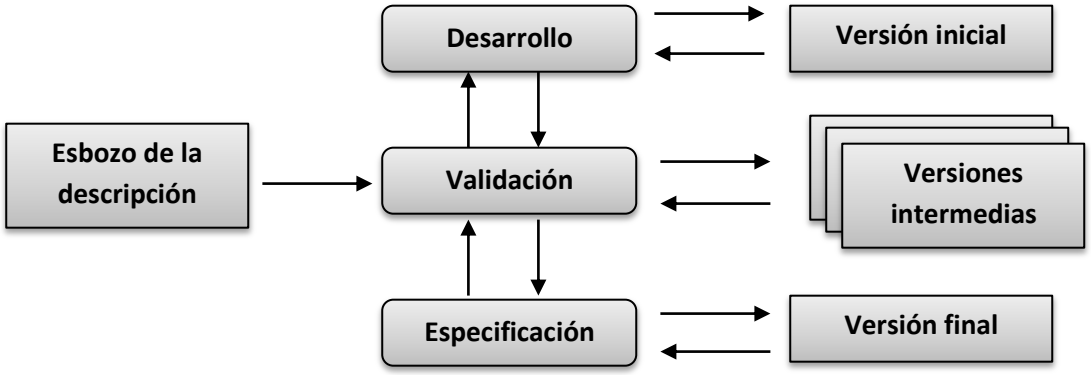
La mayor parte de los modelos de procesos del software se basan en uno de los tres modelos generales o paradigmas de desarrollo de software:

a) **El enfoque en cascada.** Considera las actividades anteriores y las representa como fases de procesos separados, tales como la especificación de requerimientos, el diseño del software, la implementación, las pruebas, etcétera. Después de que cada etapa queda definida «se firma» y el desarrollo continúa con la siguiente etapa.

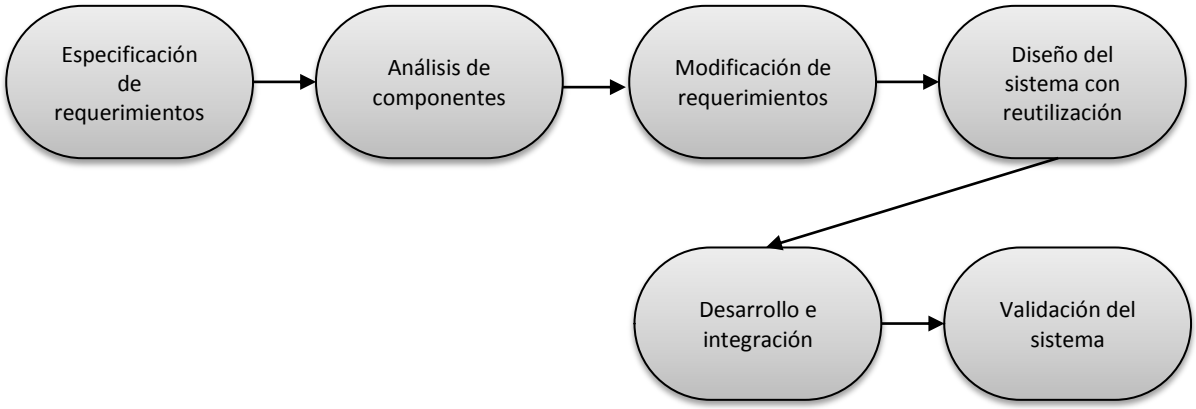


b) **Desarrollo iterativo.** Este enfoque entrelaza las actividades de especificación, desarrollo y validación. Un sistema inicial se desarrolla rápidamente a partir de especificaciones muy abstractas. Este se refina basándose en las peticiones del cliente para producir un sistema que satisfaga las necesidades de dicho cliente. El sistema puede entonces ser entregado. De forma alternativa, se puede re implementar utilizando un enfoque más estructurado para producir un sistema más sólido y mantenible.

[5]ANÁLISIS Y DISEÑO DE SISTEMAS - Kendall, Kenneth E. y Kendall, Julie, E. - 3ª. Edición



c) Ingeniería del software basada en componentes (CBSE). Esta técnica supone que las partes del sistema existen. El proceso de desarrollo del sistema se enfoca en la integración de estas partes más que desarrollarlas desde el principio.



3.2.6. Modelos ágiles de desarrollo de software[6]

Los modelos ágiles de desarrollo de software, conocidos anteriormente como metodologías livianas, intentan evitar los tortuosos y burocráticos caminos de las metodologías tradicionales enfocándose en la gente y los resultados.

[6] Tomados de METODOLOGÍAS ÁGILES, Ingeniería de software, Universidad unión bolivariana, http://ingenieriadesoftware.mex.tl/63758_AUP.html

Es un marco de trabajo conceptual de la ingeniería de software que promueve iteraciones en el desarrollo a lo largo de todo el ciclo de vida del proyecto. Existen muchos métodos de desarrollo ágil; la mayoría minimiza riesgos desarrollando software en cortos lapsos de tiempo. El software desarrollado en una unidad de tiempo es llamado una iteración, la cual debe durar de una a cuatro semanas. Cada iteración del ciclo de vida incluye: planificación, análisis de requerimientos, diseño, codificación, revisión y documentación. Una iteración no debe agregar demasiada funcionalidad para justificar el lanzamiento del producto al mercado, pero la meta es tener un demo (sin errores) al final de cada iteración. Al final de cada iteración el equipo vuelve a evaluar las prioridades del proyecto.

Los métodos Agiles enfatizan las comunicaciones cara a cara en vez de la documentación. La mayoría de los equipos Agiles están localizados en una simple oficina abierta, a veces llamadas "plataformas de lanzamiento", La oficina debe incluir revisores, diseñadores de iteración, escritores de documentación y ayuda y directores de proyecto. Los métodos ágiles también enfatizan que el software funcional es la primera medida del progreso. Combinado con la preferencia por las comunicaciones cara a cara, generalmente los métodos ágiles son criticados y tratados como "indisciplinados" por la falta de documentación técnica.

Algunas de las metodologías ágiles más usadas en el entorno laboral son:

- **Extreme Programming (XP)**
- **Scrum**
- **Agile Modeling Adaptive Software Development (ASD)**
- **Crystal Clear**
- **Dynamic Systems Development Method (DSDM)**
- **Feature Driven Development (FDD)**
- **Agile Unified Process (AUP)**

Este tipo de metodologías contradicen en muchos de sus valores a los paradigmas clásicos debido a que casi siempre en la práctica ocurre todo tipo de cambios que obligan a los desarrolladores a reenfocar un proyecto, esto por supuesto no es “culpa” del modelo de desarrollo o de una mala planeación de un equipo de trabajo sino a la naturaleza cambiante de cualquier entorno laboral (o cualquier entorno humano) donde, sin poder contar con un resultado visible rápidamente no es posible definir adecuadamente los requerimientos y siempre ocurrirán cambios inesperados.

En los enfoques de tipo ágil se resaltan las siguientes características: agilidad, simplicidad, comunicación, retroalimentación, adaptabilidad.

3.2.7. Modelo de prototipos

La excesiva lógica incremental de los modelos clásicos ha sido sustituida por paradigmas simples que buscan un resultado rápido sobre el que se pueda visualizar más fácilmente un resultado.

Los procesos de desarrollo más usados en la actualidad tienen un enfoque evolutivo, empezando con versiones básicas que van creciendo de acuerdo con los requerimientos que van apareciendo.

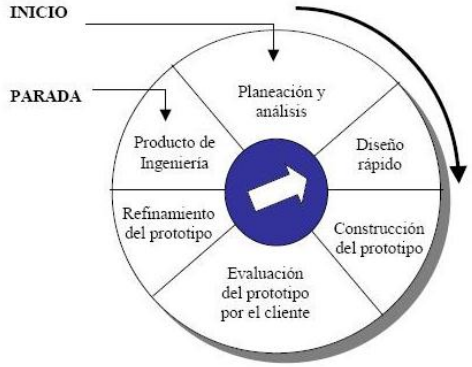


Ilustración 1: Modelo prototipos[7]

El Modelo de Prototipos dentro del paradigma de desarrollo evolutivo inicia con la definición de los objetivos globales para el software, luego se identifican los requisitos conocidos y las áreas del esquema en donde es necesaria más definición. Este modelo se utiliza para dar al usuario una vista preliminar de parte del software. Este modelo es básicamente prueba y error ya que si al usuario no le gusta una parte del prototipo significa que la prueba falló por lo cual se debe corregir el error que se tenga hasta que el usuario quede satisfecho. Además el prototipo debe ser construido en poco tiempo, usando los programas adecuados y no se debe utilizar mucho dinero pues a partir de que este sea aprobado nosotros podemos iniciar el verdadero desarrollo del software.[8]

[7] Zachman, Jhon A. *El modelado de las empresas: la arquitectura de Zachman*. Zachman Institute for Framework Advancement. Estados Unidos, 1999.
[8] Tomado de: EcuRed: *Ingeniería de software - Modelo de prototipos*, http://www.ecured.cu/Modelo_de_Prototipos

La construcción de un prototipo asegura que el software sea de mejor calidad, además de que su interfaz sea de agrado para el usuario. Un prototipo podrá ser construido solo si con el software es posible experimentar.

Etapas del modelo de prototipos

- Recolección y refinamiento de requisitos
- Modelado, diseño rápido
- Construcción del Prototipo
- Desarrollo, evaluación del prototipo por el cliente
- Refinamiento del prototipo
- Producto de Ingeniería

La construcción de un primer prototipo basado en la idea y requisitos iniciales puede ser un producto de software funcional como un diseño de ventanas, a medida de las diferentes iteraciones del modelo este prototipo ira creciendo en funcionamiento y características.

Ventajas

- Puede adaptarse a cualquier modelo sin cambiar su flujo de actividades
- Reduce el riesgo de construir productos que no satisfagan las necesidades de los usuarios.
- Reduce costo y aumenta la probabilidad de éxito.
- Exige disponer de las herramientas adecuadas (lenguaje de programación, SGBD, etc.).
- Este modelo es útil cuando se conoce los objetivos generales para el software, pero aún no existe claridad en cuanto a aspectos específicos del funcionamiento.
- Código reusable.

Tipos de modelo de prototipos:

- Modelo de Prototipos rápido: Se desarrollan rápidamente nuevos prototipos y se descarta los anteriores.
- Modelo de Prototipos reutilizable: Reutiliza el prototipo haciéndolo evolucionar desde su propuesta inicial.
- Modelo de Prototipos Modular (**Prototipos incrementales**): Un prototipo básico al que se le van agregando nuevas herramientas y funcionalidades.
- Modelo de Prototipos Horizontal: prototipo que muestra las funcionalidades que tendrá pero aun sin desarrollarse completamente.
- Modelo de Prototipos Vertical: Prototipo que cumple algunas funciones concretas

- Modelo de Prototipos de Baja-fidelidad: Prototipo económico hecho en forma de presentación donde se visualiza el resultado final sin perder tiempo en codificación.
- Modelo de Prototipos de Alta-fidelidad: Se crea un prototipo más completo capaz de cubrir la mayoría de funciones, tiene un alto costo.

Algunas de las nociones que ayudan a tomar la decisión de usar este enfoque son:

- El proyecto a abordar debe permitir experimentación
- Es un modelo para proyectos económicos
- Se desarrolla rápidamente (dependiendo del número de iteraciones)
- Para equipos de desarrollo pequeños
- Interfaz agradable e intuitiva

3.2.8. UML - Lenguaje Unificado de Modelado

El análisis de sistemas es el proceso de clasificación e interpretación de hechos, diagnóstico de problemas y manejo de la información para hacer mejoras a un sistema, siendo el diseño la fase de planificación, reemplazo o complementación de un sistema organizacional.

Para estas fases del software se han desarrollado diferentes modelos con los cuales se han obtenido resultados satisfactorios, mas no óptimos puesto que cada uno posee características diferentes con sus respectivas ventajas y desventajas sin nombrar de paso la “descentralización” de los mismos.

Es entonces cuando se plantea la necesidad de crear un mismo lenguaje que permita modelar sistemas, de manera que se pueda en cualquier momento construir software partiendo de un solo esquema de modelado, tanto estructural como orientado a objetos, es entonces cuando se desarrolla UML.

El Lenguaje Unificado de Modelado (**Unifield Modelin Language UML**), es un lenguaje estándar para escribir planos de software, UML se puede utilizar para visualizar, especificar, construir y documentar los artefactos de un sistema que involucra una gran cantidad de software. UML prescribe un conjunto de notaciones y diagramas estándar para modelar sistemas orientados a objetos, y describe la semántica esencial de lo que estos diagramas y símbolos significan.

UML es una consolidación de muchas de las notaciones y conceptos más usados en el enfoque orientados a objetos.

- Grade Booch, James Rumbaugh, e Ivar Jacobson, creadores de tres de las metodologías orientadas a objetos más populares

- 1996, el Object Management Group (OMG), publicó una petición con propósito de un **METAMODELO** orientado a objetos de semántica y notación estándares. UML, en su versión 1.0, fue propuesto como una respuesta a esta petición.

- En enero de 1997. Hubo otras cinco propuestas rivales. Durante el transcurso de 1997, los seis promotores de las propuestas, unieron su trabajo y presentaron al OMG un documento revisado de UML, llamado UML versión 1.1.

- Dicho documento fue aprobado por el OMG en Noviembre de 1997. El OMG llama a este documento OMG UML versión 1.1.

Un modelo representa a un sistema software desde una perspectiva específica, cada modelo nos permite fijarnos en un aspecto distinto del sistema.

UML está compuesta por diferentes elementos gráficos que se combinan para conformar diagramas que son utilizados para representar elementos del sistema, entre el repertorio de diagramas tenemos los siguientes:

- Diagramas de clases
- Diagramas de Objetos
- Diagrama de Casos de Uso
- Diagrama de Estados
- Diagrama de Secuencia
- Diagrama de Actividades
- Diagrama de Colaboración
- Diagrama de Componentes
- Diagrama de Distribución

3.2.9. Aplicaciones web y aplicaciones de escritorio

Una aplicación es una herramienta que fue diseñada y desarrollada para una tarea específica.

A diferencia de otros tipos de software como los de sistema o de programación, un aplicativo tiene el objetivo de cubrir las necesidades para la solución de un problema definido, ejemplo de esto son los aplicativos que permita ver imágenes, reproducir música, realizar cálculos, procesar texto, comprimir archivos, etc.

Lo más común en el entorno informático es encontrarse con aplicaciones de oficina que incluyen un sinfín de funciones para poderlas usar de diferentes formas, por ejemplo una hoja de cálculo puede servir para llevar un registro de personas, listas de inventario, registrar compras y ventas, crear gráficos, entre muchísimas otras, así en un entorno normal encontramos que un conjunto de aplicativos básicos podría potencialmente “servir para todo” pero la realidad a nivel organizacional suele ser distinta.

Los aplicativos anteriormente nombrados pueden ser útiles en muchos entornos pero debido a su naturaleza pública no están pensados para cubrir las necesidades específicas que las empresas poseen y es por esto que los programadores desarrollan continuamente toda clase de soluciones orientado a los requerimientos de un cliente o de una actividad concreta.

La creación de software es algo muy común hoy en día y dependiendo de la necesidad que se desee cubrir este puede ser un aplicativo web o un aplicativo de escritorio. Dejando de lado la base de datos podemos definir lo siguiente:

Aplicación web

Será un servidor el encargado de realizar la funcionalidad del sistema que hemos implementado a través de un programa que manejará el usuario con el navegador web (Opera, Firefox, Chrome, etc.) de su ordenador.

Entre sus ventajas se puede resaltar las siguientes:

- Disponibilidad desde cualquier lugar y dispositivo.
- Centralizado: puede actualizarse fácilmente en el servidor donde sea instalado.
- Compatibilidad: no depende del sistema operativo, pocos requerimientos

Algunas de sus desventajas más importantes están:

- Seguridad: la desventaja más importante una aplicación web estará accesible a un público mucho más grande y por tanto se

eleva exponencialmente el riesgo al que están sujetos los datos.

- Eficiencia: depende de distintos factores pero al no encontrarse físicamente en el equipo casi siempre resulta menos eficiente para ser operado.

Aplicación de escritorio

Será un programa el encargado de realizar la funcionalidad del software implementado que se debe instalar en cada puesto de trabajo. La principal ventaja de este sistema será la rapidez de uso ya se puede incorporar todos los controles de escritorio y todos los eventos asociados a ellos.

Entre sus ventajas se puede resaltar las siguientes:

- Suelen ser más robustas y estables que las aplicaciones Web.
- Rendimiento: el tiempo de respuesta es muy rápido.
- Seguridad: pueden ser muy seguras, además al no estar funcionando en línea son menos susceptibles a ataques informáticos.

Algunas de sus desventajas más importantes están:

- Acceso limitado al ordenador donde fue instalada.
- Depende del sistema operativo y de las características físicas.
- Instalación y Actualización local e individual.
- Requerimientos especiales de software instalado en el computador.

La discusión sobre si una aplicación web o una aplicación de escritorio no suele ser objeto de un gran debate, simplemente se debe pensar en la función que cumplirá el aplicativo y de acuerdo a eso escoger la opción más adecuada.

3.2.10. Lenguaje de programación PHP[9]

PHP es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Es usado principalmente en interpretación del lado del servidor (server-side scripting) pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica.

[9] Javier Gil Rubio y Jorge Tejedor Cerbel - CREACIÓN DE SITIOS WEB CON PHP

PHP es un acrónimo recursivo que significa PHP Hypertext Pre-processor (inicialmente PHP Tools, o, Personal Home Page Tools). Fue creado originalmente por Rasmus Lerdorf en 1994; sin embargo la implementación principal de PHP es producida ahora por The PHP Group y sirve como el estándar de facto para PHP al no haber una especificación formal. Publicado bajo la PHP License, la Free Software Foundation considera esta licencia como software libre.

PHP es un lenguaje interpretado de propósito general ampliamente usado y que está diseñado especialmente para desarrollo web y puede ser incrustado dentro de código HTML. Generalmente se ejecuta en un servidor web, tomando el código en PHP como su entrada y creando páginas web como salida. Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas sin costo alguno. PHP se encuentra instalado en más de 20 millones de sitios web y en un millón de servidores, aunque el número de sitios en PHP ha compartido algo de su preponderante sitio con otros nuevos lenguajes no tan poderosos desde 2005. Es también el módulo Apache más popular entre las computadoras que utilizan Apache como servidor web.

3.2.11. DBMS (en español SGBD - Sistema de Gestión de Base de Datos)

Los servidores que actúan como contenedores de los datos utilizan un tipo de software especial que automatiza los procesos de información, este software se conoce como sistema de gestión de base de datos o SGBD (DBMS).

A través del tiempo y de acuerdo a las necesidades han surgido muchos SGBD diferentes que con el avance tecnológico y los diferentes enfoques y modelos han ido incrementando sus funciones y mejorando sus características, sin embargo, eso no significa que todos sean iguales.

Si se pretende abordar la automatización de la información de una organización y se va a desarrollar una base de datos (previo diseño) es muy importante determinar cuál es el SGBD que mejor se adapta a las necesidades empresariales, el hardware disponible, la arquitectura de la red de datos de la organización, el modelo de base de datos entre otros.

Algunos de los SGBD más conocidos y sus atributos más importantes pueden verse en la siguiente tabla comparativa:

Tabla 1: Comparativa DBMS

Datos / SGBD	Creador	Lanzamiento	Licencia	Plataformas					Límite de tamaño [2]	Espacio en disco (requerimientos mínimos)[4]	Costo aproximado licencia versión estándar[5] (dólares)
								UNIX			
MySQL	MySQL AB	1996	GPL y propietario [1]	Si	Si	Si	Si	Si	65536 TB	200MB	$600
Oracle	Oracle Corporation	1977	Propietario	Si	Si	Si	Si	Si	Sin límite[3]	500MB	$15000
PostgreSQL	PostgreSQL Global Development Group	1989	Licencia BSD	Si	Si	Si	Si	Si	Sin límite[3]	100MB	Libre
Microsoft SQL server	Microsoft	1989	Propietario	No	Si	No	No	No	524272 TB	800MB	$6000
DB2	IBM	1982	Propietario	Si	Si	Si	Si	Si	Sin límite[3]	2GB	$7500

De la tabla anterior debemos tener en cuenta lo siguiente:

- ✓ El software de MySQL es gratuito siempre que se use con software GPL, sino, con software propietario tiene un costo anual de $600 a $6000 por servidor dependiendo del soporte y la versión.
- ✓ Es importante saber que el tamaño máximo de los archivos de datos de una base de datos dependen del sistema operativo. Existen varias medidas asociadas al tamaño, no solo de espacio en disco sino también de la cantidad de índices, de registros, de tablas, etc.
- ✓ En realidad todo SGBD tiene un límite de almacenaje de datos aunque este va creciendo conforme aparecen nuevas versiones, como dichos valores son tan altos normalmente no son tenidos en cuenta y se ofrecen estos sistemas como "ilimitados", por ejemplo, en su versión 10.5, DB2 ofrece un límite de 2 ExaBytes (aproximadamente 2000000 de TeraBytes).
- ✓ Tamaño mínimo requerido de espacio libre en disco para instalación del software.
- ✓ Las licencias mostradas en la tabla aplican a la versión estándar, las versiones *Enterprise* son mucho más costosas, el cobro se hace por cada servidor.

3.2.12. MySQL

MySQL (cuya sigla en inglés se traslada a My Structured Query Language o Lenguaje de Consulta Estructurado) se remite a principios de la década de 1980. Programadores de IBM lo desarrollaron para contar con un código de programación que permitiera generar múltiples y extendidas bases de datos para empresas y organizaciones de diferente tipo. Desde esta época numerosas versiones han surgido y muchas de ellas fueron de gran importancia. Hoy en día MySQL es desarrollado por la empresa Sun Mycrosystems.

Una de las características más interesantes de MySQL es que permite recurrir a bases de datos multiusuario a través de la web y en diferentes lenguajes de programación que se adaptan a diferentes necesidades y requerimientos. Por otro lado, MySQL es conocida por desarrollar alta velocidad en la búsqueda de datos e información, a diferencia de sistemas anteriores. Las plataformas que utiliza son de variado tipo y entre ellas están: LAMP, MAMP, SAMP, BAMP y WAMP

(aplicables a Mac, Windows, Linux, BSD, Open Solaris, Perl y Phyton entre otras).

Se están estudiando y desarrollando nuevas versiones de MySQL que buscan presentar mejoras y avances para permitir un mejor desempeño en toda aquella actividad que requiera el uso de bases de datos relacionales. Entre estas mejoras están: Un nuevo dispositivo de depósito y almacenamiento, backup para todos los tipos de almacenamientos, replicación segura, planificación de eventos y otras más

3.2.13. Bases de datos[10]

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. En la actualidad, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), que ofrece un amplio rango de soluciones al problema de almacenar datos.

Existen unos programas denominados sistemas gestores de bases de datos, abreviados SGBD, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada. Las propiedades de estos SGBD, así como su utilización y administración, se estudian dentro del ámbito de la informática.

3.2.14. Diseño de una base de datos

Existen distintos modos de organizar la información y representar las relaciones entre los datos en una base de datos. Los Sistemas administradores de bases de datos convencionales usan uno de los tres modelos lógicos de bases de datos para hacer seguimiento de las entidades, atributos y relaciones. Los tres modelos lógicos principalmente de bases de datos son el jerárquico, de redes y el relacional. Cada modelo lógico tiene ciertas ventajas de procesamiento y también ciertas ventajas de negocios.

- **Modelo de jerárquico de datos:** Una clase de modelo lógico de bases de datos que tiene una estructura arborescente. Un

[10]Tomado de: SISTEMAS DE BASES DE DATOS –Thomas M. Cannolly y Carolyn E. Begg - 4ª Edicion.

registro subdivide en segmentos que se interconectan en relaciones padre e hijo y muchos más. Los primeros sistemas administradores de bases de datos eran jerárquicos. Puede representar dos tipos de relaciones entre los datos: relaciones de uno a uno y relaciones de uno a muchos

- **Modelo de datos en red:** Es una variación del modelo de datos jerárquico. De hecho las bases de datos pueden traducirse de jerárquicas a en redes y viceversa con el objeto de optimizar la velocidad y la conveniencia del procesamiento. Mientras que las estructuras jerárquicas describen relaciones de muchos a muchos.
- **Modelo relacional de datos:** Es el más reciente de estos modelos, supera algunas de las limitaciones de los otros dos anteriores. El modelo relacional de datos representa todos los datos en la base de datos como sencillas tablas de dos dimensiones llamadas relaciones. Las tablas son semejantes a los archivos planos, pero la información en más de un archivo puede ser fácilmente extraída y combinada.

3.2.15. Modelo relacional

Corresponde con el modelo usado actualmente para modelar problemas de realidad y bases de datos, se propuso en el año 1970 en los laboratorios de IBM por E.F. Codd.

Este modelo consiste fundamentalmente en el uso de relaciones, representadas de forma lógica como tablas que almacenan conjuntos de datos o tuplas (las filas de una tabla) y que a su vez comparten atributos (columnas), en la siguiente ilustración se expresan estos conceptos.

Representación lógica	Representación física	Modelo relacional
Tabla	Archivo secuencial	Relación
Fila	Registro	Tupla
Columna	Campo	Atributo

Ilustración 2: Conceptos básicos modelo relacional[11]

"A diferencia de otros modelos el lugar y la forma en que se almacenen los datos no tienen relevancia, como en el modelo jerárquico y el de red, esto genera una considerable ventaja pues es

[11] Tomados de EL MODELO RELACIONAL: fundamentos del diseño de base de datos, Departamento de ciencias de la computación, Universidad de granada, http://decsai.ugr.es/.

más fácil de entender y de utilizar para un usuario esporádico de la base de datos. La información puede ser recuperada o almacenada mediante consultas, ofreciendo una amplia flexibilidad y poder para administrar la información.

Para realizar las consultas a bases de datos relacionales el lenguaje más utilizado es SQL (Structured Query Language), el cual es un estándar implementado por los principales motores o sistemas de gestión de bases de datos relacionales." [12]

3.2.16. SQL (Structured Query Language)

Es el nombre que se le da a un tipo de lenguaje pensado para la gestión de bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas en forma de consultas que, gracias al uso del álgebra facilitan la recuperación de datos de una base de datos.

El científico de IBM Edgar Frank Codd, basándose en la propuesta del modelo relacional desarrolla un sublenguaje conocido como SEQUEL (Structured English Query Language) para permitir la gestión de dicho tipo de bases y que sería el antecesor de SQL.

Tras diferentes cambios y revisiones finalmente se publica su primera versión con el nombre de SQL en 1987, a través de los años ha seguido recibiendo diferentes revisiones y cambios para adaptarse a las nuevas necesidades en lo que respecta a datos.

En esencia, el SQL es un lenguaje declarativo de alto nivel que especifica que es lo que se quiere y no como conseguirlo, es decir que una sentencia no establece un orden de ejecución. Está orientado al manejo de conjuntos de registros y no registros individuales, con lo que ofrece una elevada productividad en la codificación y en la orientación a objetos. Una sentencia de SQL puede resultar equivalente a más de un programa que emplee un lenguaje de bajo nivel.

3.2.17. La serie ISO 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

[12] Tomado de: Modulo de seguridad en base de datos, Vega, Jesús E., Universidad Abierta y a Distancia UNAD, 2013

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.
- ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR.
  Otros países donde también está publicada en español son, por ejemplo, Colombia y Venezuela. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

- 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. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en

Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

- ISO 27003: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009.
  Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ISO 27004: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- ISO 27005: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2008.
  Consistirá en una guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Recogerá partes de ISO/IECTR 13335.

- ISO 27006: Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI's) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI's. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010.
  Consistirá en una guía de auditoría de un SGSI.

- ISO 27011: En fase de desarrollo; su fecha prevista de publicación es Enero de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- ISO 27031: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010.
  Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- ISO 27032: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

- ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028.

3.2.18. ISO/IEC 27001

El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques – Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.
Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002.

Actualmente el ISO-27001 es el único estándar aceptado internacionalmente (Certificable) para la administración de la

seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

3.2.19. Objetivos Controles de la norma ISO 27001 (V. 2013) [13]

- **Política de seguridad A5**
  Una política de seguridad es un enunciado formal de las reglas y procedimientos que los usuarios que acceden a los recursos de la organización deben cumplir, para prevenir, proteger y manejar los riesgos, y su objetivo es de informar al mayor nivel de detalle a los usuarios, empleados y gerentes, de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

- **Organización de la seguridad de la información A6**
  La organización de la seguridad está orientada a administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades. Además de fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

- **Gestión de activos A8**
  La gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad. Además de definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

- **Seguridad de los recursos humanos A7**
  La seguridad de los recursos humanos este orientado a reducir los riesgos de error humano, robo, fraude, o uso inadecuado de las instalaciones, además de definiciones de puestos de trabajo y asignación de recursos. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

[13] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001, Icontec internacional, 11-12-2013

- La seguridad de los recursos humanos también debe garantizar que los usuarios estén al tanto de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la política de seguridad de la información de la organización en el transcurso de sus tareas normales.

- **Seguridad física y del entorno A11**
  La seguridad física y del entorno está destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

  Además debe controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo. Y también debe implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

- **Seguridad de las operaciones A12**
  La seguridad de las operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información así como de la información que se transmite de los diferentes riesgos asociados generalmente a eventos técnicos.

- **Seguridad de las comunicaciones A13**
  La seguridad de las comunicaciones está orientada a garantizar la seguridad en la transferencia de información y el tratamiento de los datos.

- **Control de acceso A9**
  Un sistema de control de acceso es el que impide el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. También Implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Además debe registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- **Criptografía A10**
  La criptografía cuenta con su propio control en esta versión de la norma, tiene como objetivo asegurar el uso adecuado de las técnicas de criptografía para proteger las características de seguridad de la información: Confidencialidad, Autenticidad e integridad a través de políticas y gestión de claves.

- **Gestión de los incidentes de la seguridad de la información A16**
  La gestión de los incidentes de la seguridad de la información está orientada a minimizar el daño producido por incidentes y anomalías en materia de seguridad, donde también se determina como monitorear dichos incidentes y aprender de los mismos, para no repetir fallos o interrupciones del mismo tipo.

- **Adquisición, desarrollo y mantenimiento de sistemas A14**
  El desarrollo y mantenimiento de sistemas de información está orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento. Además de definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan y también determina los métodos de protección de la información crítica o sensible.

- **Relaciones con los proveedores A15**
  Busca asegurar la protección de activos de forma que sean accesibles a los proveedores por medio de políticas de cumplimiento y acuerdos que establezcan un tratamiento de riesgos, niveles de acceso entre otros.

- **Aspectos de seguridad de la información en la gestión de continuidad del negocio A17**
  La gestión de la continuidad del negocio está orientada a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres. Además de asegurar la coordinación con el personal de la organización y los contactos externos que participaran en

las estrategias de planificación de contingencias y asignarles funciones para cada actividad definida.

- **Cumplimiento A18**
  El cumplimiento está destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos y de los requisitos de seguridad además de revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

3.2.19.1. Modelo de procesos "*Planear-Hacer-Verificar-Actuar*"

Esta norma adopta el modelo de procesos "Planear-Hacer-Verificar-Actuar" (PHVA) que se aplica para estructurar los procesos del SGSI, este toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y, a través de acciones y procesos necesarios produce resultados de seguridad de la información que cumplen con dichos requisitos y expectativas.

La adopción del modelo PHVA refleja los principios establecidos en las directrices OCDE para la seguridad de sistemas y redes de información, esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

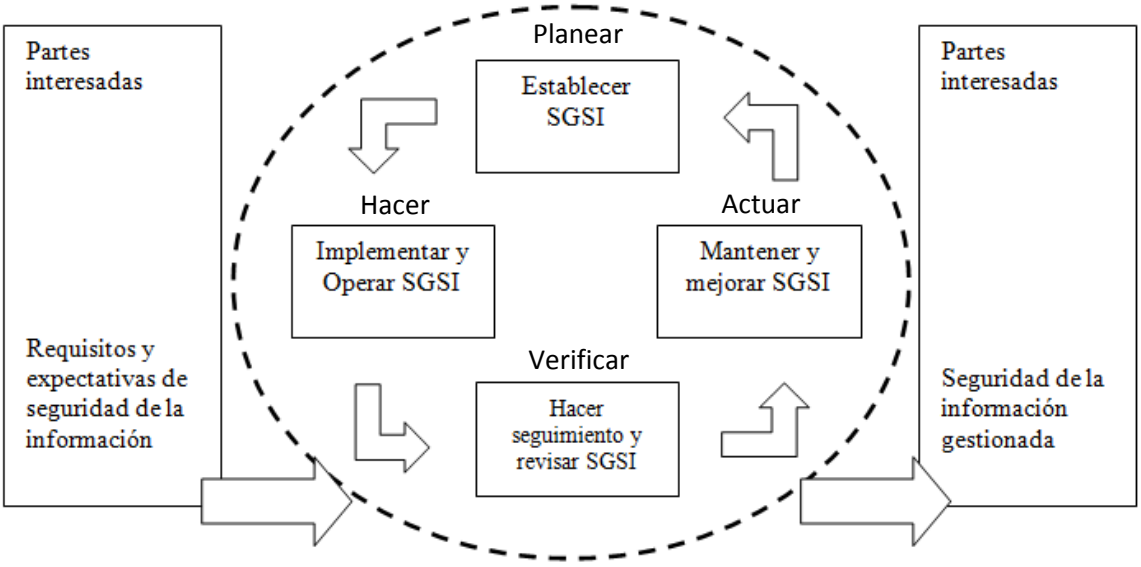


Ilustración 3: Modelo PHVA aplicado a los procesos de SGSI[14]

Tabla 2: Descripción del modelo PHVA

Proceso PHVA	Descripción
Planificar: Establecer el SGSI	Establecer la politica, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las politicas y objetivos globales de una organización.
Hacer: Implementar y operar el SGSI	Implementar y operar la politica, los controles, procesos y procedimientos del SGSI
Verificar: hacer seguimiento y revisar el SGSI	Evluar, y, en donde sea apliucable, medir el desempeño del proceso contra la politica y los objetivos de seguridad y la experiencia practica y reportar los resultados a la direccion para su revisión.
Actuar: Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoria interna del SGSI y la revision por la direccion para lograr la mejora continua.

[14]Figura tomada de ICONTEC, 2006, COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, www.Icontec.org.co.

3.2.20. ISO/IEC 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Al igual que ISO 17799 tampoco es una norma certificable sino que recomienda a las organizaciones una serie de medidas que les ayuden a mejorar la seguridad de la información y generar políticas para su esquema de seguridad cobijando todos los aspectos básicos.

La ISO/IEC 27002 cuenta con 11 dominios, 39 objetivos de control y 133 controles descritos en la siguiente tabla:

Tabla 3: Dominios, objetivos de control y controles ISO/IEC 27002[15]

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES
1. POLÍTICA DE SEGURIDAD.	**1.1.** Política de seguridad de la información.	**1.1.1.** Documento de política de seguridad de la información. **1.1.2.** Revisión de la política de seguridad de la información.
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**2.1.** Organización interna	**2.1.1.** Compromiso de la Dirección con la seguridad de la información. **2.1.2.** Coordinación de la seguridad de la información. **2.1.3.** Asignación de responsabilidades relativas a la seg. de la información. **2.1.4.** 6.1.4 Proceso de autorización de recursos para el tratamiento de la **2.1.5.** información. **2.1.6.** 6.1.5 Acuerdos de confidencialidad. **2.1.7.** 6.1.6 Contacto con las autoridades.

[15] Información tomada de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

		2.1.8. Contacto con grupos de especial interés. **2.1.9.** Revisión independiente de la seguridad de la información.
	2.2. Tratamiento	**2.2.1.** Identificación de los riesgos derivados del acceso de terceros. **2.2.2.** Tratamiento de la seguridad en la relación con los clientes. **2.2.3.** Tratamiento de la seguridad en contratos con terceros.
3. GESTIÓN DE ACTIVOS	**3.1.** Responsabilidad sobre los activos.	**3.1.1.** Inventario de activos. **3.1.2.** Propiedad de los activos. **3.1.3.** Uso aceptable de los activos.
	3.2. Clasificación de la información.	**3.2.1.** Directrices de clasificación. **3.2.2.** Etiquetado y manipulado de la información.

4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**4.1.** Antes del empleo.	**4.1.1.** Funciones y responsabilidades. **4.1.2.** Investigación de antecedentes. **4.1.3.** Términos y condiciones de contratación.
	4.2. Durante el empleo.	**4.2.1.** Responsabilidades de la Dirección. **4.2.2.** Concienciación, formación y capacitación en seg. de la informac. **4.2.3.** Proceso disciplinario.
	4.3. Cese del empleo o cambio de puesto de trabajo.	**4.3.1.** Responsabilidad del cese o cambio. **4.3.2.** Devolución de activos. **4.3.3.** Retirada de los derechos de acceso.
5. SEGURIDAD FÍSICA Y DEL ENTORNO.	**5.1.** Áreas seguras.	**5.1.1.** Perímetro de seguridad física. **5.1.2.** Controles físicos de entrada. **5.1.3.** Seguridad de oficinas, despachos e instalaciones. **5.1.4.** Protección contra las amenazas externas y de origen ambiental. **5.1.5.** Trabajo en áreas seguras. **5.1.6.** Áreas de acceso público y de carga y descarga.
	5.2. Seguridad de los equipos.	**5.2.1.** Emplazamiento y protección de equipos. **5.2.2.** Instalaciones de suministro. **5.2.3.** Seguridad del cableado. **5.2.4.** Mantenimiento de

		los equipos. **5.2.5.** Seguridad de los equipos fuera de las instalaciones. **5.2.6.** Reutilización o retirada segura de equipos. **5.2.7.** Retirada de materiales propiedad de la empresa.
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	**6.1.** Responsabilidades y procedimientos de operación.	**6.1.1.** Documentación de los procedimientos de operación. **6.1.2.** Gestión de cambios. **6.1.3.** Segregación de tareas. **6.1.4.** Separación de los recursos de desarrollo, prueba y operación.
	6.2. Gestión de la provisión de servicios por terceros.	**6.2.1.** Provisión de servicios. **6.2.2.** Supervisión y revisión de los servicios prestados por terceros. **6.2.3.** Gestión del cambio en los servicios prestados por terceros.
	6.3. Planificación y aceptación del sistema.	**6.3.1.** Gestión de capacidades. **6.3.2.** Aceptación del sistema.
	6.4. Protección contra el código malicioso y descargable.	**6.4.1.** Controles contra el código malicioso. **6.4.2.** Controles contra el código descargado en el cliente.
	6.5. Copias de seguridad.	**6.5.1.** Copias de seguridad de la información.
	6.6. Gestión de la seguridad de las redes.	**6.6.1.** Controles de red. **6.6.2.** Seguridad de los servicios de red.

	6.7. Manipulación de los soportes.	**6.7.1.** Gestión de soportes extraíbles. **6.7.2.** Retirada de soportes. **6.7.3.** Procedimientos de manipulación de la información. **6.7.4.** Seguridad de la documentación del sistema.
	6.8. Intercambio de información.	**6.8.1.** Políticas y procedimientos de intercambio de información. **6.8.2.** Acuerdos de intercambio. **6.8.3.** Soportes físicos en tránsito. **6.8.4.** Mensajería electrónica. **6.8.5.** Sistemas de información empresariales.
	6.9. Servicios de comercio electrónico.	**6.9.1.** Comercio electrónico. **6.9.2.** Transacciones en línea. **6.9.3.** Información públicamente disponible.
	6.10. Supervisión.	**6.10.1.** Registros de auditoría. **6.10.2.** Supervisión del uso del sistema. **6.10.3.** Protección de la información de los registros. **6.10.4.** Registros de administración y operación. **6.10.5.** Registro de fallos. **6.10.6.** Sincronización del reloj.

7. CONTROL DE ACCESO.	**7.1.** Requisitos de negocio para el control de acceso.	**7.1.1.** Política de control de acceso
	7.2. Gestión de acceso de usuario.	**7.2.1.** Registro de usuario. **7.2.2.** Gestión de privilegios. **7.2.3.** Gestión de contraseñas de usuario. **7.2.4.** Revisión de los derechos de acceso de usuario.
	7.3. Responsabilidades de usuario.	**7.3.1.** Uso de contraseña. **7.3.2.** Equipo de usuario desatendido. **7.3.3.** Política de puesto de trabajo despejado y pantalla limpia. **7.3.4.**
	7.4. Control de acceso a la red.	**7.4.1.** Política de uso de los servicios en red. **7.4.2.** Autenticación de usuario para conexiones externas. **7.4.3.** Identificación de los equipos en las redes. **7.4.4.** Protección de los puertos de diagnóstico y configuración remotos. **7.4.5.** Segregación de las redes. **7.4.6.** Control de la conexión a la red. **7.4.7.** Control de encaminamiento (routing) de red. **7.4.8.**
	7.5. Control de acceso al sistema operativo	**7.5.1.** Procedimientos seguros de inicio de sesión. **7.5.2.** Identificación y

		autenticación de usuario. **7.5.3.** Sistema de gestión de contraseñas. **7.5.4.** Uso de los recursos del sistema. **7.5.5.** Desconexión automática de sesión. **7.5.6.** Limitación del tiempo de conexión.
	7.6. Control de acceso a las aplicaciones y a la información.	**7.6.1.** Restricción del acceso a la información. **7.6.2.** Aislamiento de sistemas sensibles.
	7.7. Ordenadores portátiles y teletrabajo.	**7.7.1.** Ordenadores portátiles y comunicaciones móviles. **7.7.2.** Teletrabajo.
8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**8.1.** Requisitos de seguridad de los sistemas de información.	**8.1.1.** Análisis y especificación de los requisitos de seguridad. **8.1.2.**
	8.2. Tratamiento correcto de las aplicaciones.	**8.2.1.** Validación de los datos de entrada. **8.2.2.** Control del

		procesamiento interno. **8.2.3.** Integridad de los mensajes. **8.2.4.** Validación de los datos de salida.
	8.3. Controles criptográficos.	**8.3.1.** Política de uso de los controles criptográficos. **8.3.2.** Gestión de claves.
	8.4. Seguridad de los archivos de sistema.	**8.4.1.** Control del software en explotación. **8.4.2.** Protección de los datos de prueba del sistema. **8.4.3.** Control de acceso al código fuente de los programas.
	8.5. Seguridad en los procesos de desarrollo y soporte.	**8.5.1.** Procedimientos de control de cambios. **8.5.2.** Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. **8.5.3.** Restricciones a los cambios en los paquetes de software. **8.5.4.** Fugas de información. **8.5.5.** Externalización del desarrollo de software.
	8.6. Gestión de la vulnerabilidad técnica.	**8.6.1.** Control de las vulnerabilidades técnicas.
9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**9.1.** Notificación de eventos y puntos débiles de seguridad de la **9.2.** información.	**9.2.1.** Notificación de los eventos de seguridad de la información. **9.2.2.** Notificación de puntos débiles de seguridad.

	9.3. Gestión de incidentes y mejoras de seguridad de la información.	**9.3.1.** Responsabilidades y procedimientos. **9.3.2.** Aprendizaje de los incidentes de seguridad de la información. **9.3.3.** Recopilación de evidencias.
10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**10.1.** Aspectos de seguridad de la información en la gestión de la **10.2.** continuidad del negocio.	**10.2.1.** Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. **10.2.2.** Continuidad del negocio y evaluación de riesgos. **10.2.3.** Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. **10.2.4.** Marco de referencia para la planificación de la cont. del negocio. **10.2.5.** Pruebas, mantenimiento y reevaluación de planes de continuidad.
11. CUMPLIMIENTO.	**11.1.** Cumplimiento de los requisitos legales.	**11.1.1.** Identificación de la legislación aplicable. **11.1.2.** Derechos de propiedad intelectual (DPI). **11.1.3.** Protección de los documentos de la organización. **11.1.4.** Protección de datos y privacidad de

		la información de carácter personal. **11.1.5.** Prevención del uso indebido de recursos de tratamiento de la información. **11.1.6.** Regulación de los controles criptográficos.
	11.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.	**11.2.1.** Cumplimiento de las políticas y normas de seguridad. **11.2.2.** Comprobación del cumplimiento técnico.
	11.3. Consideraciones sobre las auditorías de los sistemas de información.	**11.3.1.** Controles de auditoría de los sistemas de información. **11.3.2.** Protección de las herramientas de auditoría de los sist. de inform.

3.2.21. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática,

estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

3.2.22. ESTABLECIMIENTO Y GESTIÓN DEL SGSI[16]

La organización es la principal protagonista y a través de su junta directiva designar él o los responsables del control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos, además deberá:

a) Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

b) Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, los activos y tecnología.

c) Definir el enfoque organizacional para la valoración del riesgo.

d) Identificar los riesgos.

e) Analizar y evaluar los riesgos.

f) Identificar y evaluar las opciones para el tratamiento de los riesgos.

g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.

h) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

i) Obtener autorización de la dirección para implementar y operar el SGSI.

j) Elaborar una declaración de aplicabilidad que incluya:

[16]Tomados de ICONTEC, 2006, COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, pág. 21.

- Los objetivos de control y los controles seleccionados y las razones para su selección.
- Los objetivos de control y controles implementados actualmente.
- La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión.

3.2.23. IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI[17]

La organización debe:

a) Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados que incluyen considerar la financiación y la asignación de funciones y responsabilidades.

c) Implementar los controles seleccionados para cumplir los objetivos de control.

d) Definir cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar como se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.

e) Implementar programas de formación y de toma de conciencia.

f) Gestionar la operación del SGSI.

g) Gestionar los recursos del SGSI.

h) Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

3.2.24. SEGUIMIENTO Y REVISIÓN DEL SGSI[18]

[17]Tomados de ICONTEC, 2006, COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, pág. 23.

La organización debe:

a) Ejecutar procedimientos de seguimiento y revisión y otros controles para:
   - Detectar rápidamente errores en los resultados del procesamiento;
   - Identificar con prontitud los incidentes e intentos de violación a la seguridad que tuvieron éxito como los que fracasaron;
   - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
   - Ayudar a detectar eventos de seguridad y de esta manera impedir incidentes de seguridad mediante el uso de indicadores y
   - Determinar si las acciones tomadas para solucionar un problema de violación de seguridad fueron eficaces.

b) Emprender revisiones regulares de la eficacia del SGSI teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

d) Revisar las valoraciones de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable identificado teniendo en cuenta cambios en
   - La organización,
   - La tecnología,
   - Los objetivos y procesos de negocio, las amenazas identificadas, la eficacia de los controles implementados y eventos externos tales como cambios en el entorno legal o reglamentario en las obligaciones contractuales y en el clima social.

e) Realizar auditorías internas del SGSI a intervalos planificados.

[18]Tomados de ICONTEC, 2006, COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, pág. 24.

f) Emprender una revisión del SGSI realizada por la dirección en forma regular para asegurar que el alcance siga siendo suficiente y que identifiquen mejoras al proceso de SGSI.

g) Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.

h) Registrar acciones y eventos que podría tener impacto en la eficacia o el desempeño del SGSI.

3.2.25. MANTENIMIENTO Y MEJORA DEL SGSI[19]

La organización debe, regularmente:

a) Implementar las mejoras identificadas en el SGSI;

b) Emprender las acciones correctivas y preventivas adecuadas. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.

c) Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente llegar a acuerdos sobre cómo proceder.

d) Asegurar que las mejoras logran los objetivos previstos.

[19]Tomados de ICONTEC, 2006, COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, pág. 25.

3.3. MARCO CONCEPTUAL

3.3.1. Seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas, reactivas y correctivas que permiten mantener la calidad de la información en sus tres pilares: Integridad, Disponibilidad y Confidencialidad (conocidos también como CIA por sus siglas).

El campo de la seguridad de la información es bastante amplio y ha venido creciendo desde la segunda guerra mundial principalmente por el uso de diferentes tecnologías que permiten su tratamiento y que al mismo tiempo deben someterse a diferentes medidas que garanticen la calidad de la información, de ahí nace también la seguridad informática que es el conjunto de medidas cuyo fin es similar (mantener los tres pilares de la información) pero enfocándose en el aspecto tecnológico.

La seguridad de la información no es algo que pueda alcanzarse o lograrse de manera completa sino que es un proceso continuo que debe mantenerse y adaptarse para evitar convertir las vulnerabilidades en riesgos.

3.3.2. Integridad

Es una de las propiedades de la información que describe la “exactitud” de la información, es decir, que la información no ha sufrido ninguna modificación no autorizada y se mantiene igual desde su origen hasta su lectura.

Si una persona no autorizada ingresara al sistema de información de una empresa y modificara la información de un registro se estaría vulnerando esta propiedad, para este tipo de riesgos existen diferentes tipos de medidas preventivas entre las que se destaca la firma digital.

3.3.3. Disponibilidad

Otra característica o condición de la información es la disponibilidad, se dice que la información posee esta propiedad cuando puede ser accedida y obtenida en completitud en cualquier momento que se requiera, es decir, que la información sea accesible.

Las tecnologías han hecho que el acceso a la información sea fácil y rápido, lo que hace unos años requería de una intensa consulta de archivos físicos hoy puede hacerse por distintos medios (tablets,

PDA's, teléfonos inteligentes, etc.) lo cual ha expandido este atributo y eliminado muchas de sus limitantes a costo de ampliar sus riesgos.

Uno de los riesgos más grandes relacionados con la disponibilidad en el campo de la informática son los ataques de denegación de servicio sumado a los diferentes fallos tanto de software o hardware a los que está sujeto la tecnología.

Para garantizar la disponibilidad y disminuir los riesgos existen todo tipo de medidas como centros de datos con plantas de energía independientes, servidores espejo, replicación de datos, redes de almacenamiento, enlaces redundantes, etc. Dependiendo de los costos que una organización esté dispuesta a asumir y la importancia que la disponibilidad suponga para la misma.

3.3.4. Confidencialidad

La información puede permanecer inalterada y ser accesible a quien necesite, pero si al mismo tiempo alguien sin los permisos adecuados puede acceder de forma clandestina a la información esta propiedad se pierde.

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Existen muchísimas formas de vulnerar la confidencialidad de la información desde métodos de ingeniería social, shoulder surfing[20], hasta métodos más complejos como un ataque de inyección SQL[21] para obtener credenciales de acceso.

3.3.5. Riesgo-Vulnerabilidad-Amenaza

Existen muchos conceptos que se engloban en el campo de la seguridad de la información, entre ellos los más comunes son riesgo, vulnerabilidad y amenaza, los cuales podrían tomarse erróneamente como sinónimos, pero en este contexto su diferencia es clave.

3.3.5.1. Riesgo

[20] *Dentro de la seguridad informática, esta técnica consiste en la observación directa (de una pantalla de pc de algún empleado por ejemplo) para obtener información delicada como contraseñas o datos financieros.*

[21] *Inyección SQL es una técnica que consiste en enviar cadenas de texto a un sistema las cuales son capaces de explotar vulnerabilidades pudiendo obligar a la base de datos del mismo a revelar información delicada.*

Simboliza un hecho inesperado, no calculado o no planeado que tiene un origen, que puede provocar la alteración del resultado de un conjunto de actividades y que genera unas pérdidas. De acuerdo con lo anterior los riesgos se pueden clasificar como:

- Financieros. Organización – causa – peligro.
- Dinámicos. Factores externos en constante cambio
- Estáticos. Factor humano.
- Especulativos. Posibilidad de pérdida o ganancia
- Puros. Situaciones específicas con posibilidades de pérdida o ganancia
- Fundamentales. impersonales
- Particulares. Evento particular

El riesgo está asociado a un peligro o una posibilidad de pérdida, cuando se habla de que existe una posibilidad de que hay un factor latente (quizá incontrolable) puede afectar un sistema se dice que existe una amenaza.

3.3.5.2. Amenaza

Según el efecto que ésta presente puede ser clasificada así:

- Intercepción. Acceso a una parte del sistema
- Modificación. Cambio de valores o datos
- Interrupción. Mal funcionamiento de un proceso
- Generación. Adición de elementos externos al sistema con fines maliciosos

Además dependiendo del origen de la misma se clasifica como

- Natural.
- Intencionada.
- Involuntaria.

3.3.5.3. Vulnerabilidad

¿Porque existe una amenaza? Precisamente porque no existe un sistema perfecto, todo sistema tiene algún defecto donde un hecho puede provocar pérdidas, dicho “defecto en la armadura” se conoce como vulnerabilidad y existen diferentes tipos:

- Física.
- Natural.
- Humana.
- Hardware y software.

- Medios.
- Emanación. (Señales inalámbricas que pueden interceptarse)
- Comunicaciones.

Si un riesgo se hiciera realidad el resultado será un conjunto de pérdidas asociadas a ese hecho (personas, insumos, información, redes inalámbricas, software, hardware), a los elementos que están expuestos a los riesgos se les conoce como elementos de riesgo, si estos son medidos y asociados a un riesgo en particular se tiene un riesgo especifico y si se calcula el total de pérdidas causadas por el conjunto de riesgos se obtiene un riesgo total.

3.3.6. Control informático

Cuando se habla de riesgos informáticos y de su impacto no se está hablando de “incendios” que deben “apagarse”, se está hablando de la necesidad de que existan medios para mantener a un sistema lo más seguro posible durante toda su vida útil aprovechando las ventajas de las TI, minimizando los riesgos.

Es decir, que la seguridad informática es un elemento siempre presente que se requiere para asegurar la calidad de la información. En este sentido se habla de control, mantener controlada una situación implica que se encuentre constantemente vigilada.

Un control es un conjunto de normas, técnicas, acciones y procedimientos que mantienen una organización segura, actuando en consecuencia de sus objetivos.

Un ambiente de control es el resultado de la ejecución de buenos controles y asegura que todos los elementos de la organización estén conscientes de la importancia de mantener unos niveles estables de seguridad para lo cual es necesario la aplicación de una serie de actividades como constante monitoreo, valoración, comunicación, entre otros.

Hoy en día las empresas cuentan con una gran variedad de herramientas de software para control informático, integran diferentes servicios de control para diferentes contextos (educación, salud, financiero, etc.) algunas de estas herramientas son incluso gratuitas.

La seguridad informática no solo puede ser asegurada por software. El control completo informático incluye un cambio de actitud, inclusión de nuevas herramientas y por supuesto algunos cambios en la política laboral.

Las políticas, a diferencia de otros muchos aspectos organizacionales, son importantes porque pertenecen al más alto nivel y para realizar cambios en ellas se requiere de una concientización a nivel gerencial, se clasifican en políticas Laborales, de hardware y de software. Las políticas de seguridad informática son definidas en conjunto por directivos y los encargados de los sistemas informáticos.

3.3.7. Modelo de madurez

El enfoque de los Modelos de Madurez para el control sobre los procesos de TI consiste en desarrollar un método de asignación de puntos para que una organización pueda calificarse desde Inexistente hasta Optimizada (de 0 a 5).

Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Cualquiera sea el modelo, las escalas no deben estar demasiado simplificadas, lo que haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable.

La escala del modelo de madurez es la siguiente:

- **0 Inexistente:** Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
- **1 Inicial:** Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.
- **2 Repetible:** Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.
- **3 Definida:** Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin

embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

- **4 Administrada:** Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.
- **5 Optimizada:** Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

3.3.8. Tipos de Controles[22]

3.3.8.1. Controles Preventivos

Reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones
Sistemas de claves de acceso

3.3.8.2. Controles Detectivos

No evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.
Ejemplo: Archivos y procesos que sirvan como pistas de auditoría
Procedimientos de validación

3.3.8.3. Controles Correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre

[22] Gerencie.com, (2013), Auditoría de Sistemas, Consultado en: http://www.gerencie.com/tipos-de-riesgos-de-auditoria.html

los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

3.3.9. Software

Muchas personas asocian el término software con los programas de computadora. Sin embargo, en una definición más amplia, el software no son sólo programas, sino todos los documentos asociados y la configuración de datos que se necesitan para hacer que estos programas operen de manera correcta. Por lo general, un sistema de software consiste en diversos programas independientes, archivos de configuración que se utilizan para ejecutar estos programas, un sistema de documentación que describe la estructura del sistema, la documentación para el usuario que explica cómo utilizar el sistema y sitios web que permitan a los usuarios descargar la información de productos recientes.

Los ingenieros de software se concentran en el desarrollo de productos de software, es decir, software que se vende a un cliente. Existen dos tipos de productos de software:

Productos genéricos. Son sistemas aislados producidos por una organización de desarrollo y que se venden al mercado abierto a cualquier cliente que le sea posible comprarlos.

Ejemplos de este tipo de producto son el software para PCs tales como bases de datos, procesadores de texto, paquetes de dibujo y herramientas de gestión de proyectos.

Productos personalizados (o hechos a medida). Son sistemas requeridos por un cliente en particular. Un contratista de software desarrolla el software especialmente para ese cliente. Ejemplos de este tipo de software son los sistemas de control para instrumentos electrónicos, sistemas desarrollados para llevar a cabo procesos de negocios específicos y sistemas de control del tráfico aéreo.

Una diferencia importante entre estos diferentes tipos de software es que, en los productos genéricos, la organización que desarrolla el software controla su especificación. La especificación de los productos personalizados, por lo general, es desarrollada y controlada por la organización que compra el software. Los desarrolladores de software deben trabajar con esa especificación.

No obstante, la línea de separación entre estos tipos de productos se está haciendo cada vez más borrosa. Cada vez más compañías de software empiezan con un sistema genérico y lo adaptan a las necesidades de un cliente en particular, un sistema complejo y con muchas funciones puede adaptarse a una compañía incorporando información sobre reglas de negocio y de procesos, informes, etcétera.

3.3.10. Proceso de software

Un proceso del software es un conjunto de actividades y resultados asociados que producen un pro-duelo de software. Estas actividades son llevadas a cabo por los ingenieros de software.

Existen cuatro actividades fundamentales de que son comunes para todos los procesos del software. Estas actividades son:

- **Especificación** del software donde los clientes e ingenieros definen el software a producir y las restricciones sobre su operación.
- **Desarrollo** del software donde el software se diseña y programa.
- **Validación** del software donde el software se prueba para asegurar que cumple con los requerimientos del cliente.
- **Evolución** del software donde el software se modifica para adaptarlo a los cambios requeridos por el cliente y el mercado.

Diferentes tipos de sistemas necesitan diferentes procesos de desarrollo. Por ejemplo, el software de tiempo real en un avión tiene que ser completamente especificado antes de que empiece el desarrollo, mientras que en un sistema de comercio electrónico, la especificación y el programa normalmente son desarrollados juntos. Por lo tanto, estas actividades genéricas pueden organizarse de diferentes formas y describirse en diferentes niveles de detalle para diferentes tipos de software.

3.3.11. Requerimientos

Los requerimientos para un sistema son la descripción de los servicios proporcionados por el sistema y sus restricciones operativas. Estos requerimientos reflejan las necesidades de los clientes de un sistema que ayude a resolver algún problema como el control de un dispositivo, hacer un pedido o encontrar información. El proceso de descubrir, analizar, documentar y verificar estos servicios y restricciones se denomina ingeniería de requerimientos (RE).

El término requerimiento no se utiliza de una forma constante en la industria de software.

En algunos casos, un requerimiento es simplemente una declaración abstracta de alto nivel de un servicio que debe proporcionar el sistema o una restricción de éste. En el otro extremo, es una definición detallada y formal de una función del sistema.

Si una compañía desea establecer un contrato para un proyecto de desarrollo de software grande, debe definir sus necesidades de una forma suficientemente abstracta para establecer a partir de ella una solución. Los requerimientos deben redactarse de tal forma que varios contratistas pueden licitar el contrato, ofreciendo, quizás, formas diferentes de cumplir las necesidades de los clientes en la organización. Una vez que el contrato se asigna, el contratista debe redactar una definición del sistema para el cliente más detalladamente de forma que éste comprenda y pueda validar lo que hará el software. Ambos documentos se pueden denominar documento de requerimientos para el sistema.

Algunos de los problemas que surgen durante el proceso de ingeniería de requerimientos son resultado de no hacer una clara separación entre estos diferentes niveles de descripción.

Aquí se distinguen utilizando la denominación requerimientos del usuario para designar los requerimientos abstractos de alto nivel, y requerimientos del sistema para designar la descripción detallada de lo que el sistema debe hacer. Los requerimientos del usuario y del sistema se pueden definirse así:

- Los requerimientos del usuario son declaraciones, en lenguaje natural y en diagramas, de los servicios que se espera que el sistema proporcione y de las restricciones bajo las cuales debe funcionar.

- Los requerimientos del sistema establecen con detalle las funciones, servicios y restricciones operativas del sistema. El documento de requerimientos del sistema (algunas veces denominado especificación funcional) debe ser preciso. Debe definir exactamente qué es lo que se va a implementar. Puede ser parte del contrato entre el comprador del sistema y los desarrolladores del software.

3.3.12. Prototipo de software

Un prototipo se define como "…un modelo del comportamiento del sistema que puede ser usado para entenderlo completamente o ciertos aspectos de él y así clarificar los requerimientos… Un prototipo es una representación de un sistema, aunque no es un sistema completo, posee las características del sistema final o parte de ellas"

Los prototipos son herramientas muy útiles en el desarrollo de software y traen ventajas tanto a los desarrolladores como al cliente, al poder este último ver mejor representado el producto deseado y de esta manera proponer mejor los requerimientos sobre los que debe continuarse su construcción.

La definición de prototipo es bastante amplia si pensamos que este puede ser desde un simple diseño de ventanas hasta un producto software de calidad que implementa las funciones básicas del sistema final.

Los tipos de prototipos y las distintas formas en que puede abordarse un desarrollo basado en prototipos se describe mejor en el punto **3.2.7** de este documento. Para el proyecto presente será usado un tipo de prototipo reutilizable evolutivo de acuerdo con el modelo de prototipos incrementales que se desarrollará de manera horizontal ya que el aspecto vertical del desarrollo tiene más que ver con la norma ISO/IEC 27001 de 2013.

3.4. MARCO LEGAL

- **Ley 1273 de 2009.**

  Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, como penas de prisión de 120 meses y multa de hasta 1500 salarios mínimos legales mensuales vigentes. La ley castiga los atentados contra la confidencialidad, la integridad y la confidencialidad de los datos y de los sistemas informáticos, entre otras infracciones como hurto por medios informáticos y semejantes, transferencia no consentida de activos y circunstancias de mayor unidad (ANDRADE 2009).

- **Ley 1581 de 2012 y del Decreto 1377 de 2013,**

  Por la cual se dictan disposiciones generales para la protección de datos personales. La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C–748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión, en adelante tratamiento por parte de entidades de naturaleza pública y privada. Como Ley Estatutaria (ley de especial jerarquía), tiene como fin esencial salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección.

- **Decreto 1151 de 2008.**

  Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.

- **Ley 872 de 2003 (diciembre 30)**

  Diario Oficial No. 45.418, de 2 de enero de 2004

PODER PÚBLICO - RAMA LEGISLATIVA
Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.

EL CONGRESO DE COLOMBIA DECRETA:

ARTÍCULO 1o. CREACIÓN DEL SISTEMA DE GESTIÓN DE LA CALIDAD. Créase el Sistema de Gestión de la calidad de las entidades del Estado, como una herramienta de gestión sistemática y transparente que permita dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios a cargo de las entidades y agentes obligados, la cual estará enmarcada en los planes estratégicos y de desarrollo de tales entidades. El sistema de gestión de la calidad adoptará en cada entidad un enfoque basado en los procesos que se surten al interior de ella y en las expectativas de los usuarios, destinatarios y beneficiarios de sus funciones asignadas por el ordenamiento jurídico vigente.
ARTÍCULO 2o. ENTIDADES Y AGENTES OBLIGADOS. El sistema de gestión de la calidad se desarrollará y se pondrá en funcionamiento en forma obligatoria en los organismos y entidades del Sector Central y del Sector Descentralizado por servicios de la Rama Ejecutiva del Poder Público del orden Nacional, y en la gestión administrativa necesaria para el desarrollo de las funciones propias de las demás ramas del Poder Público en el orden nacional. Así mismo en las Corporaciones Autónomas Regionales, las entidades que conforman el Sistema de Seguridad Social Integral de acuerdo con lo definido en la Ley 100 de 1993, y de modo general, en las empresas y entidades prestadoras de servicios públicos domiciliarios y no domiciliarios de naturaleza pública o las privadas concesionarios del Estado.
PARÁGRAFO 1o. La máxima autoridad de cada entidad pública tendrá la responsabilidad de desarrollar, implementar, mantener, revisar y perfeccionar el Sistema de Gestión de la Calidad que se establezca de acuerdo con lo dispuesto en la presente ley. El incumplimiento de esta disposición será causal de mala conducta.
PARÁGRAFO 2o. Las Asambleas y Concejos podrán disponer la obligatoriedad del desarrollo del Sistema de Gestión de la Calidad en las entidades de la administración central y descentralizada de los departamentos y municipios.
PARÁGRAFO TRANSITORIO. Las entidades obligadas a aplicar el Sistema de Gestión de la Calidad, contarán con un término máximo de cuatro (4) años

a partir de la expedición de la reglamentación contemplada en el artículo 6 de la presente ley para llevar a cabo su desarrollo.

ARTÍCULO 3o. CARACTERÍSTICAS DEL SISTEMA. El Sistema se desarrollará de manera integral, intrínseca, confiable, económica, técnica y particular en cada organización, y será de obligatorio cumplimiento por parte de todos los funcionarios de la respectiva entidad y así garantizar en cada una de sus actuaciones la satisfacción de las necesidades de los usuarios.

PARÁGRAFO. Este Sistema es complementario a los sistemas de control interno y de desarrollo administrativo establecidos por la Ley 489 de 1998.

El Sistema podrá integrarse al Sistema de Control Interno en cada uno de sus componentes definidos por el Departamento Administrativo de la Función Pública, de acuerdo con las políticas adoptadas por el Presidente de la República.

ARTÍCULO 4o. REQUISITOS PARA SU IMPLEMENTACIÓN. Para dar cumplimiento a lo dispuesto en la presente ley, las entidades deben como mínimo:

a) Identificar cuáles son sus usuarios, destinatarios o beneficiarios de los servicios que presta o de las funciones que cumple; los proveedores de insumos para su funcionamiento; y determinar claramente su estructura interna, sus empleados y principales funciones;
b) Obtener información de los usuarios, destinatarios o beneficiarios acerca de las necesidades y expectativas relacionadas con la prestación de los servicios o cumplimiento de las funciones a cargo de la entidad, y la calidad de los mismos;
c) Identificar y priorizar aquellos procesos estratégicos y críticos de la entidad que resulten determinantes de la calidad en la función que les ha sido asignada, su secuencia e interacción, con base en criterios técnicos previamente definidos por el Sistema explícitamente en cada entidad;
d) Determinar los criterios y métodos necesarios para asegurar que estos procesos sean eficaces tanto en su operación como en su control;
e) Identificar y diseñar, con la participación de los servidores públicos que intervienen en cada uno de los procesos y actividades, los puntos de control sobre los riesgos de mayor probabilidad de ocurrencia o que generen un impacto considerable en la satisfacción de las necesidades y expectativas de calidad de los usuarios o destinatarios, en las materias y funciones que le competen a cada entidad;
f) Documentar y describir de forma clara, completa y operativa, los procesos identificados en los literales anteriores, incluyendo todos los puntos de control.

Solo se debe documentar aquello que contribuya a garantizar la calidad del servicio;

g) Ejecutar los procesos propios de cada entidad de acuerdo con los procedimientos documentados;

h) Realizar el seguimiento, el análisis y la medición de estos procesos;

i) Implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de estos procesos.

PARÁGRAFO 1o. Este sistema tendrá como base fundamental el diseño de indicadores que permitan, como mínimo, medir variables de eficiencia, de resultado y de impacto que faciliten el seguimiento por parte de los ciudadanos y de los organismos de control, los cuales estarán a disposición de los usuarios o destinatarios y serán publicados de manera permanente en las páginas electrónicas de cada una de las entidades cuando cuenten con ellas.

PARÁGRAFO 2o. Cuando una entidad contrate externamente alguno de los procesos involucrados en el Sistema de Gestión de Calidad, deberá asegurar la existencia de control de calidad sobre tales procesos.

ARTÍCULO 5o. FUNCIONALIDAD. El sistema debe permitir:

a) Detectar y corregir oportunamente y en su totalidad las desviaciones de los procesos que puedan afectar negativamente el cumplimiento de sus requisitos y el nivel de satisfacción de los usuarios, destinatarios o beneficiarios;

b) Controlar los procesos para disminuir la duplicidad de funciones, las peticiones por incumplimiento, las quejas, reclamos, denuncias y demandas;

c) Registrar de forma ordenada y precisa las estadísticas de las desviaciones detectadas y de las acciones correctivas adoptadas;

d) Facilitar control político y ciudadano a la calidad de la gestión de las entidades, garantizando el fácil acceso a la información relativa a los resultados del sistema;

e) Ajustar los procedimientos, metodologías y requisitos a los exigidos por normas técnicas internacionales sobre gestión de la calidad.

ARTÍCULO 6o. NORMALIZACIÓN DE CALIDAD EN LA GESTIÓN. En la reglamentación del sistema de gestión de la calidad el Gobierno Nacional expedirá, dentro de los doce (12) meses siguientes a la entrada en vigencia de la presente ley, una norma técnica de calidad en la gestión pública en la que podrá tener en cuenta las normas técnicas internacionales existentes sobre la materia.

La norma técnica expedida por el Gobierno deberá contener como mínimo disposiciones relativas a:

1. Los requisitos que debe contener la documentación necesaria para el funcionamiento del sistema de gestión de calidad, la cual incluye la definición de la política y objetivos de calidad, manuales de procedimientos y calidad necesarios para la eficaz planificación, operación y control de procesos, y los requisitos de información que maneje la entidad.
2. Los mínimos factores de calidad que deben cumplir las entidades en sus procesos de planeación y diseño.
3. Los controles de calidad mínimos que deben cumplirse en la gestión de Recursos Humanos y de infraestructura.
4. Los controles o principios de calidad mínimos que deben cumplirse en el desarrollo de la función o la prestación del servicio y en los procesos de comunicación y atención a usuarios destinatarios.
5. Las variables mínimas de calidad que deben medirse a través de los indicadores que establezca cada entidad, en cumplimiento del parágrafo 1o del artículo 4 de esta ley.
6. Los requisitos mínimos que debe cumplir toda entidad en sus procesos de seguimiento y medición de la calidad del servicio y de sus resultados.
7. Los objetivos y principios de las acciones de mejoramiento continuo y las acciones preventivas y correctivas que establezcan cada entidad.

En ningún caso el decreto que expida la norma técnica podrá alterar ni desarrollar temas relativos a la estructura y funciones de la administración, al régimen de prestación de servicios públicos, al estatuto general de contratación de la administración pública, ni aspectos que pertenezcan a la competencia legislativa general del Congreso. Cada entidad definirá internamente las dependencias y funcionarios que de acuerdo con sus competencias deban desarrollar el Sistema de Gestión de la Calidad, sin que ello implique alteración de su estructura o tamaño.

ARTÍCULO 7o. CERTIFICACIÓN DE CALIDAD. Una vez implementado el sistema y cuando la entidad considere pertinente podrá certificar su Sistema de Gestión de la Calidad con base en las normas internacionales de calidad.

PARÁGRAFO 1o. El Gobierno Nacional diseñará los estímulos y reconocimientos de carácter público a las entidades que hayan implementado su sistema de gestión de calidad y publicará periódicamente el listado de entidades que hayan cumplido con lo establecido en la presente ley.

PARÁGRAFO 2o. Ninguna de las entidades de las diferentes Ramas del Poder Público podrá contratar con un organismo externo el proceso de certificación del Sistema de Gestión de la Calidad, cuando exista una entidad

gubernamental de orden nacional con experiencia en este tipo de procesos de certificación.
ARTÍCULO 8o. APOYO ESTATAL. Durante el desarrollo del sistema de gestión de calidad y su posterior certificación, la Escuela Superior de Administración Pública, ESAP, el Servicio Nacional de Aprendizaje, SENA, el Departamento Administrativo de la Función Pública y demás instituciones de orden distrital y nacional que dentro de su ordenamiento jurídico deban garantizar la eficiencia y el buen desarrollo de la función pública brindarán el apoyo a que hubiere lugar prestando el debido acompañamiento a las entidades que así lo soliciten.
ARTÍCULO 9o. VIGENCIA. La presente ley rige a partir de la fecha de su publicación.

- **Copyright**

  En el Derecho anglosajón se utiliza la noción de copyright (traducido literalmente como derecho de copia) que, por lo general, comprende la parte patrimonial de los derechos de autor.
  El derecho de autor se basa en la idea de un derecho personal del autor, fundado en una forma de identidad entre el autor y su creación. El derecho moral está constituido como emanación de la persona del autor: reconoce que la obra es expresión de la persona del autor y así se le protege. La protección del copyright se limita estrictamente a la obra, sin considerar atributos morales del autor en relación con su obra, excepto la paternidad; no lo considera como un autor propiamente tal, pero tiene derechos que determinan las modalidades de utilización de una obra

  Para Colombia los derechos de autor están reguladas por:

  - ✓ Ley 23 de 1982
  - ✓ Ley 44 de 1993
  - ✓ Ley 1032 de 2006

  El objeto de estas normas es proteger las obras artísticas, científicas y literarias que pueden ser reproducidas o divulgadas de cualquier forma, así como amparar los derechos de los artistas, intérpretes, productores de fonogramas y titulares de programas de computador (software). La protección de los trabajos artísticos y literarios no depende de su registro, y por lo tanto la omisión de éste no es obstáculo para que goce de salvaguarda, ya que la titularidad de la obra se obtiene con la creación de la misma, mas no con su registro. Sin embargo, se recomienda el registro de la obra ante la Dirección Nacional de Derechos de Autor, de manera que pueda oponerse como

defensa frente a las reproducciones no autorizadas, ya que constituye un eficaz medio de prueba del derecho que facilita su negociación y defensa judicial. La ley 1032 del 2006 modifico la pena por el delito de violación a los derechos patrimoniales de autor y derechos conexos incrementándose de 2 a 4 años (antiguo régimen) a 4 a 8 años (nuevo régimen).

- **Licencia pública general de GNU**

  La Licencia Pública General de GNU (GNUGPL, por sus siglas en inglés) es una licencia libre y gratuita con derecho de copia para software y otros tipos de obras. Las licencias para la mayoría del software y otras obras de índole práctica están diseñadas para privarle de la libertad para distribuir y modificar las obras. Por el contrario, la Licencia Pública General de GNU garantiza la libre distribución y modificación de todas las versiones de un programa, a fin de asegurarle dicha libertad a todos los usuarios.

  Todos los derechos que se otorgan conforme a esta Licencia se otorgan por el término del copyright que ampara al Programa y son irrevocables siempre y cuando se cumplan las condiciones establecidas. Esta Licencia lo autoriza en forma expresa e ilimitada a ejecutar el Programa sin modificaciones. El producto obtenido a partir de la ejecución de una obra amparada está cubierto por esta Licencia únicamente si el producto, dado su contenido, constituye una obra amparada. Esta Licencia reconoce sus derechos de uso razonable y otros equivalentes, conforme a las leyes de copyright.

  Se puede crear, ejecutar y propagar obras amparadas que no transmita, sin condiciones en la medida en que su licencia siga vigente de alguna otra manera. Se puede transmitir obras amparadas a terceros con el único fin de que éstos realicen modificaciones exclusivamente el creador del software, o que le proporcionen los medios para ejecutar dichas obras, siempre y cuando se cumpla con los términos de esta Licencia en lo que respecta a la transmisión de cualquier material que exceda su control del copyright. Aquéllos que de esta manera creen o ejecuten las obras aparadas, deben hacerlo exclusivamente en su nombre, bajo su dirección y control y sobre la base de términos que les prohíban hacer copias de su material protegido por derechos de autor fuera de la relación que mantienen con usted.

- **Norma ISO-IEC/27001.**

  Define como organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es

posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.[23]

[23] www.iso27001standard.com/

4. CAPITULO 4: DISEÑO METODOLÓGICO

4.1. FASES DE DESARROLLO

Para la elaboración de este estudio se seguirán las siguientes fases a nivel general:

4.1.1. Fase 1: Recolección de información.

Contextualización con la norma ISO/IEC 27001 y cambios de la norma con respecto a su versión de 2005.
Buscar metodologías de implementación, casos y antecedentes
Clasificación de información recolectada en grupos de importancia o relevancia para el proyecto.

4.1.2. Fase 2: Análisis.

Determinar los requerimientos de usuario en cuanto a las funcionalidades
Determinar los indicadores para la medición de cada uno de los dominios y objetivos de control
Determinar los reportes que sean necesarios y que deba generar el software de acuerdo a los requerimientos

4.1.3. Fase 3: Diseño y desarrollo.

Diseñar los cuestionarios para la lista de chequeo que servirá para medición de la seguridad en cada uno de los dominios
Diseñar la base de datos que soporte el sistema de acuerdo a las necesidades de los usuarios
Diseñar la interfaz para que sea de fácil manejo para los usuarios del software
Seleccionar el lenguaje apropiado para la implementación de la herramienta de software para que corra en entornos web
Desarrollar cada una de las funcionalidades del software para ponerlo a prueba

4.1.4. Fase 4: Validación y pruebas.

Realizar las pruebas de validación de la herramienta software para evitar errores por parte de los usuarios
Realizar pruebas para montar la aplicación en un servidor y que permita realizar la evaluación desde lugares remotos.
Realizar la prueba en una empresa específica para determinar el estado actual de la organización en cuanto a seguridad y las recomendaciones para establecer un SGSI adecuado a sus necesidades.

4.1.5. Fase 5: Documentación y recomendaciones.

Elaborar el informe final de los resultados de la prueba del software Realizar la entrega del informe y realizar la sustentación de la aplicación del software

4.2. DESCRIPCIÓN GENERAL DE ACTIVIDADES

El desarrollo de este proyecto se regirá según el orden de actividades, tareas y tiempo descrito en la siguiente tabla:

Tabla 4: Descripción general de actividades del presente proyecto

ACTIVIDADES	TIEMPO
1. Recolección de Información	**5 Semanas**
a) Contextualización con la norma ISO/IEC 27001 y cambios de la norma con respecto a su versión de 2005.	2 Semanas
b) Buscar metodologías de implementación, casos y antecedentes	2 Semanas
c) Clasificación de información recolectada en grupos de importancia o relevancia para el proyecto.	1 Semana
2. Análisis	**6 Semanas**
d) Determinar los requerimientos de usuario en cuanto a las funcionalidades	2 Semanas
e) Determinar los indicadores para la medición de cada uno de los dominios y objetivos de control	2 Semanas
f) Determinar los reportes que sean necesarios y que deba generar el software de acuerdo a los requerimientos	2 Semanas
3. Diseño y desarrollo	**10 Semanas**
g) Diseñar los cuestionarios para la lista de chequeo que servirá para medición de la seguridad en cada uno de los dominios	2 Semanas
h) Diseñar la base de datos que soporte el sistema de acuerdo a las necesidades de los usuarios	1 Semana
i) Diseñar la interfaz para que sea de fácil manejo para los usuarios del software	2 Semanas
j) Seleccionar el lenguaje apropiado para la implementación de la herramienta de software para que corra en entornos web	1 Semana
k) Desarrollar cada una de las funcionalidades del software para ponerlo a prueba	4 Semanas
4. Validación y pruebas	**4 Semanas**

l) Realizar las pruebas de validación de la herramienta software para evitar errores por parte de los usuarios.	1 Semana
m) Realizar pruebas para montar la aplicación en un servidor y que permita realizar la evaluación desde lugares remotos.	1 Semana
n) Realizar la prueba en una empresa específica para determinar el estado actual de la organización en cuanto a seguridad y las recomendaciones para establecer un SGSI adecuado a sus necesidades.	2 Semanas
5. Documentación final y recomendaciones	**3 Semanas**
o) Elaborar el informe final, guías y resultados de la prueba del software.	2 Semanas
p) Realizar la entrega del informe y realizar la sustentación de la aplicación del software.	1 Semana

4.3. METODOLOGÍA DE LA INVESTIGACIÓN

El proyecto se enmarca en un **ENFOQUE CUANTITATIVO**, ya que se van a cuantificar las diversas propiedades de las variables del proyecto, así mismo esta es una investigación de **TIPO DESCRIPTIVO** ya que medirá las variables para generar datos objetivos. Además la investigación tiene un diseño no experimental y transversal, ya que se estudian las variables en un corte de tiempo definido, en donde se determinó la manera más adecuada de medir dicho conjunto de variables para poder dar una visión general del estado de los controles de seguridad de la información y si estos cumplen con la norma ISO/IEC 27001 de 2013 o al menos si son lo suficientemente fuertes para conservar la calidad de la información, también cómo y en que se iba a desarrollar la herramienta para el tratamiento de los datos que se evalúan.

4.3.1. MODELO DE DESARROLLO

Tomando como referencia lo descrito en el marco teórico y teniendo en cuenta las ventajas del modelo de prototipos será usado el tipo de modelo **Prototipos Incrementales (ver 3.2.7)**, recordando que una de las grandes ventajas del mismo es la rapidez y la capacidad de generar resultados que pueden ser revisados a medida que se desarrollan nuevas funcionalidades y avances, además el uso del lenguaje de programación Java permite que dichos prototipos puedan ser reutilizados.

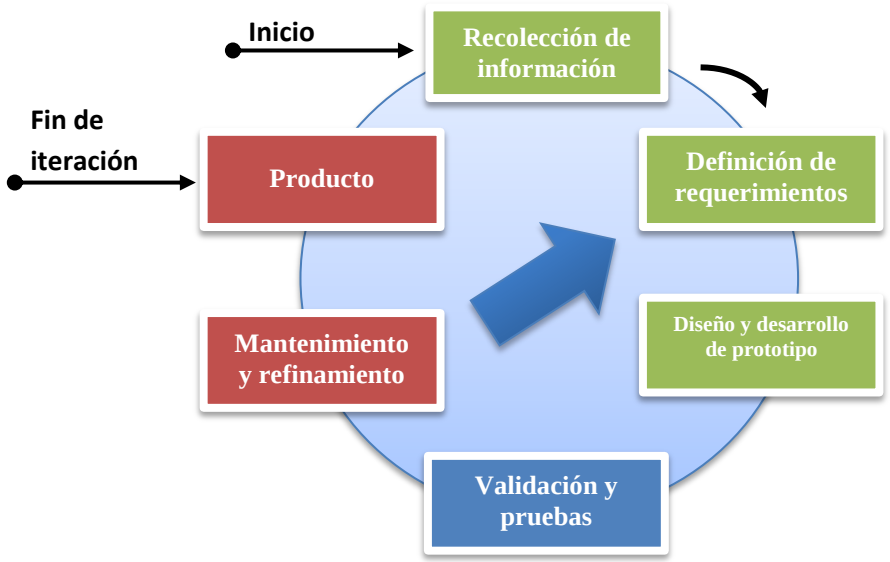


Ilustración 4: Modelo Prototipo Incremental del proyecto

5. CAPÍTULO 5: EJECUCIÓN DEL PROYECTO

5.1. ANTECEDENTES ISO 27001:2005 - ISO 27001:2013

Recordemos en primer lugar, ISO 27001 es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa. Puede ser implementada en cualquier tipo de organización de cualquier tamaño con o sin fines de lucro y ha sido un esfuerzo combinado de los mejores especialistas del mundo en seguridad informática en busca de generalizar la forma en que las organizaciones mantienen segura su información.

Una característica que diferencia esta norma de otras de la misma familia, dedicadas al tema de la seguridad informática, es que las organizaciones pueden certificarse bajo la misma, teniendo un plus ante sus clientes.

La versión de la norma ISO 27001 de 2005 estuvo en revisión por parte de la Organización Internacional de Estandarización ISO en el año 2013 en la cual participaron importantes empresas de distintos sectores así como representantes de 43 países.

Esta norma está diseñada para ajustarse a las necesidades que van apareciendo en el ámbito de la seguridad informática por lo que se prevé posteriores actualizaciones. La revisión de 2013 corresponde con la primera revisión de esta norma y propone una importante cantidad de cambios, desde el orden y aparición de controles hasta el uso de nuevos conceptos y definiciones.

5.1.1. ESTRUCTURA DE LA NUEVA VERSIÓN ISO 27001:2013

La siguiente estructura obedece a los lineamientos del anexo SL[24] de ISO/IEC siguiendo una serie de lineamientos estandarizados para el desarrollo documental sin importar su enfoque, la estructura de la versión 2013 es la siguiente:

[24] "Suplemento Consolidado de las Directivas ISO/IEC"

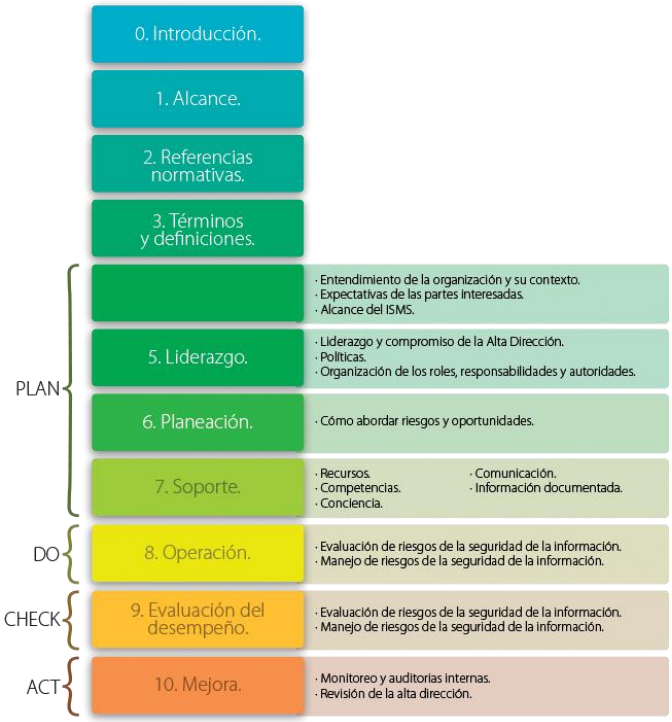


Ilustración 5: estructura ISO 27001:2013[25]

5.1.2. PROPUESTA ACTUALIZADA DE LOS OBJETIVOS DE CONTROL

El “Anexo A – Referencia de objetivos y controles” continúa formando parte de este estándar, pero los anexos “B” y “C” se han eliminado.

Una mejor organización de los controles de la norma busca ajustarse mejor a las necesidades reales de una organización, en la siguiente imagen puede apreciarse mejor el orden de los controles

[25] Tomada de: ISO-27001:2013 ¿Qué hay de nuevo?, Dulce González Trejo. ISO-27001 e ITIL, 2013, http://www.magazcitum.com.mx/?p=2397#.VjvKH7cvfIU

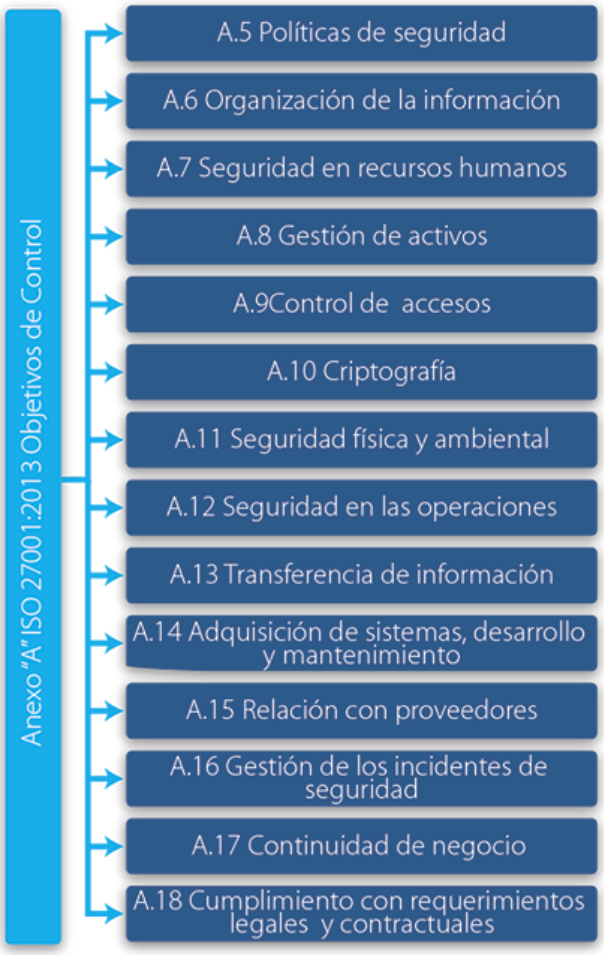


Ilustración 6: Anexo "A" ISO 27001: 2013

Así mismo los cambios de los objetivos de control con respecto a su versión de 2005 pueden apreciarse en la siguiente tabla.

Tabla 5: Cambios de controles ISO 27001

Anexo A ISO 27001:2005	Anexo A ISO 27001:2013
A.5 Política de Seguridad	A.5 Políticas de Seguridad
A.6 Organización de seguridad de la información	A.6 Organización de la seguridad de la información
A.8 Seguridad en recursos humanos	A.7 Seguridad en recursos humanos
A.7 Administración de activos	A.8 Administración de activos
A.11 Control de acceso	A.9 Control de acceso
	A.10 Criptografía
A.9 Seguridad física y ambiental	A.11 Seguridad física y ambiental
A.10 Administración de comunicaciones y operaciones	A.12 Seguridad en operaciones
	A.13 Seguridad en comunicaciones
A.12 Adquisición, desarrollo y mantenimiento de sistemas	A.14 Adquisición, desarrollo y mantenimiento de sistemas
	A.15 Relación con proveedores
A.13 Administración de incidentes de seguridad de la información	A.16 Administración de incidentes de seguridad de la información
A.14 Administración de continuidad del negocio	A.17 Aspectos de seguridad de la información en la administración de continuidad del negocio
A.15 Cumplimiento	A.18 Cumplimiento

Los cambios expuestos reflejan las necesidades de adaptación de la norma a las nuevas tecnologías y pretenden una mayor facilidad en su implementación, sin embargo en este proyecto no se pretende ahondar en más detalles sobre los cambios específicos que ha sufrido la norma ya que se aleja de los objetivos del proyecto, la intención de este apartado de información es simplemente la de entrar en contexto, explorar algunas de las nuevas características de la norma y hacer énfasis en la flexibilidad e importancia de este estándar.

5.1.3. EVALUACIÓN DE CONTROLES Y ESTADISTICAS

ISO/IEC 27001 establece los objetivos de control y controles de referencia que deben cumplirse para poder alcanzar una certificación, pero más importante es alcanzar un nivel óptimo de seguridad de la información, para ello existe en esta familia de normas la ISO/IEC 27002 donde se establece para cada uno de los controles las recomendaciones o mejores prácticas para lograr el cumplimiento del control.

5.1.3.1. NIVEL DE MADUREZ EN LA SEGURIDAD DE LA INFORMACIÓN

La evaluación de la norma depende básicamente del cumplimiento de los controles. Aunque pueden existir diferentes formas de establecer, optimizar y madurar cada control las disposiciones recomendadas están propuestas por la ISO 27002, de aquí se parte entonces que, en cumplimiento de cada recomendación puede decirse que se alcanza el cumplimiento del control.

Básicamente para cumplir con cada control se debe evaluar cada recomendación. Esto es realizado por el personal que cada organización designe para esta tarea o por consultores externos y se realizará de forma periódica (al menos una vez al año) de forma que se mantenga un nivel adecuado de seguridad.

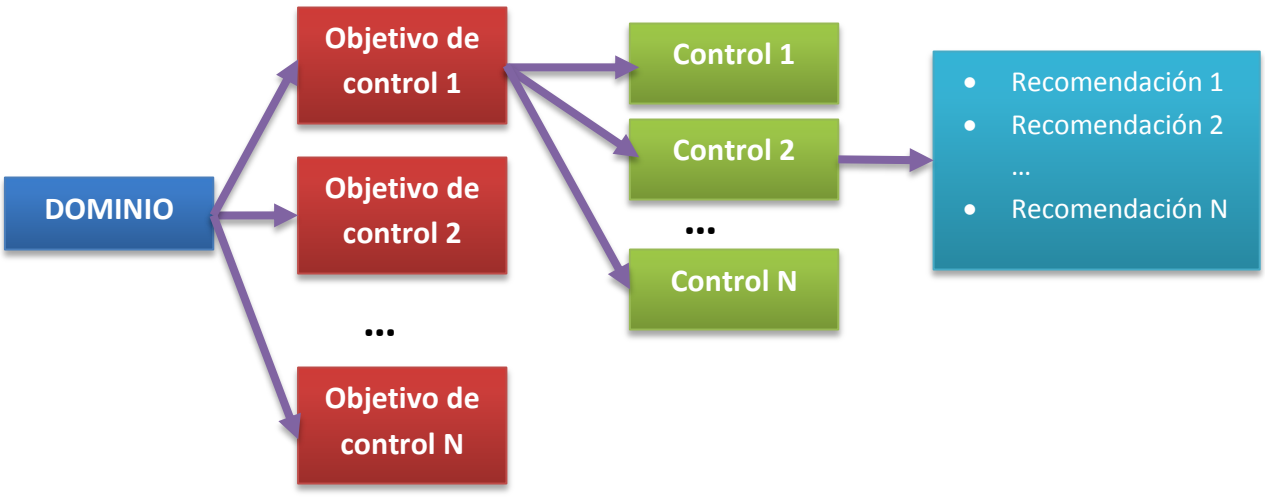


Ilustración 7: Esquema básico de división controles ISO 27001 y 27002

La división observada en el anterior esquema da una idea general de cómo trabaja el software con respecto a ambas normas, básicamente se calificarán los controles mediante el cumplimiento de sus recomendaciones haciendo uso del modelo de madurez descrito en el punto 3.3.7 de este documento.

Calificando cada recomendación como un aspecto a cumplir y en qué nivel de madurez se encuentra dicha actividad recomendada se puede verificar el nivel de madurez del control.

0. Inexistente
1. Inicial
2. Repetible
3. Definida
4. Administrada
5. Optimizada

Así mismo se obtendrá el nivel de madurez de cada OBJETIVO DE CONTROL y DOMINIO a través del desarrollo completo de todos sus controles e incluso se puede inferir un nivel de madurez general de una organización en cuanto a la seguridad de la información.

5.1.3.2. CARACTERISTICAS DE LA CALIDAD DE LA INFORMACIÓN

En segundo lugar se evalúan las características de la calidad de la información. Esta información no está disponible en las normas anteriormente nombradas, sin embargo el software basa dicha evaluación en el Anexo 2: "*ISO27k_Controls_cross_check*" El cual es un documento que puede obtenerse de forma gratuita en los foros del sitio web www.ISO27001security.com donde a través de la opinión y experiencia de distintos expertos en el tema se clasifica cada control de acuerdo con el impacto que este tiene en cada característica de seguridad:

- ✓ **Persuasión:** El control reduce la amenaza al persuadir a los piratas informáticos de atacar el sistema.
- ✓ **Evación:** El control reduce el impacto al evadir la situación que representa riesgo.
- ✓ **Prevención:** El control reduce la vulnerabilidad, la mayoría de controles de seguridad cumplen esta característica.

- ✓ **Detección:** El control ayuda a detectar a tiempo un evento o incidente de seguridad.
- ✓ **Reacción:** El control ayuda a reducir el impacto de un incidente que se materialice al ofrecer una reacción oportuna.
- ✓ **Recuperación:** El control ayuda a reducir el impacto de incidentes con medidas para regresar al funcionamiento normal o por medio de copias de seguridad.

Los controles, además de contar con estas características también se clasifican según el objetivo de calidad de la información que ayudan a mantener.

- ✓ **Confidencialidad.**
- ✓ **Integridad.**
- ✓ **Disponibilidad.**

En el mismo anexo se especifica que los controles pueden estar clasificados de cualquier otra forma, sin embargo es un excelente punto de inicio y será útil para dar una visión tanto de las características como de los objetivos de calidad, de los cuales también se obtendrá unos valores basados en el nivel de cada control solo que en lugar de usar el modelo de madurez se usará una escala porcentual.

Con estos elementos se puede ofrecer un conjunto de resultados que ayuden a la organización a visualizar su estado en cuanto a la seguridad de la información con base en la norma ISO/IEC 27001 y además ayudará a promover mejores prácticas en busca de una certificación o simplemente de mejorar la calidad de su actividad.

5.2. DISEÑO DEL SOFTWARE

El presente proyecto está encaminado a buscar una forma dinámica de medir o calificar el nivel de cumplimiento e implementación de controles en un SGSI (sistema de gestión de seguridad de la información) según la norma ISO/IEC 27001 de 2013.

Es de conocimiento general que un proceso de auditoría es un trabajo bastante complejo y más aún si se hace en busca de una certificación internacional requiere del consentimiento y apoyo de todos los niveles de una organización así como de tiempo suficiente para verificar cada particularidad existente.

La presente solución de software no busca profundizar en cada aspecto de una auditoría informática, pues como se ha expresado no resulta práctico si lo que se necesita es saber de la forma más inmediata posible cuales son las mayores fortalezas y debilidades, el interés de este proyecto es ofrecer un producto que pueda mostrar a grandes rasgos el estado de un SGSI de cualquier organización basado en el estado de sus controles, calificando cada aspecto y ofreciendo respuestas gráficas así como descripciones y ayudas tomada de la misma norma.

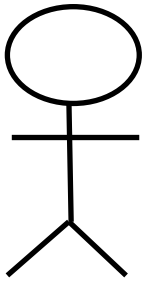
Esto servirá en principio como punto de partida en la implementación del SGSI así como en la obtención de apoyo de la dirección y de las partes comprometidas ya que sus resultados serán de fácil interpretación. Posteriormente, durante el proceso de mejora del SGSI el software tendrá dos funciones, en primer lugar dinámicamente registrará los avances en la aplicación de controles y registro de hallazgos, segundo, permitirá administrar más fácilmente este proceso de forma que no se omitan puntos de la norma.

5.2.1. INGENIERIA DE REQUERIMIENTOS

5.2.1.1. Identificación de actores

Aunque dentro del proceso de auditoría intervienen muchas partes, el manejo del software se realizara por un solo tipo de actor, este usuario corresponde con la o las personas encargadas de registrar los avances en el establecimiento del sistema de seguridad.

Tabla 6: Actores del proyecto

ACTOR	DESCRIPCIÓN	ACTIVIDADES
 USUARIO	Operador del software, cualquier persona o personas dentro de la organización que se encarga de registrar los avances del SGSI	• Ingreso al software • Creación de proyecto y credenciales. • Valoración de controles • Ingreso de hallazgos • Consulta • Generación de reportes del software • Actualización de la información

5.2.1.2. Requerimientos funcionales

- **Gestión de proyecto (Nuevo, Abrir, Guardar, Editar):** Para poder usar todas las características del software será necesario crear un proyecto o seleccionar uno ya creado que contendrá información básica sobre la organización para fines descriptivos. Gracias a este enfoque el software podrá abarcar la información de varias auditorías o de distintas organizaciones como ayuda o para fines comparativos.

  Los proyectos estarán protegidos por credenciales que pueden ser editadas en el apartado de “Proyecto” así como las demás características del mismo.
- **Vista general de estadísticas:** El software permite ver en principio las estadísticas del proyecto: controles pendientes, porcentaje de avance y nivel general de cumplimiento.
- **Controles:** En el módulo de controles se podrá encontrar el listado de controles y ver el avance de cada uno.
- **Cuestionarios:** Cada control cuenta con su respectivo cuestionario que permitirá evaluar los avances calificándolos según su avance en porcentaje.
- **Hallazgos:** Cada control contendrá un cuadro que permite describir los hallazgos que podrán ser consultados o gestionados según sea pertinente.
- **Resultados:** Este módulo permite ver los datos de los avances sobre cada control, puede ser editado para ver

resultados de un objetivo de control hasta del proyecto completo.

- **Generador de reporte:** Similar al módulo de resultados permitirá editar el tipo de resultados que se desea reportar y con ello generar un archivo de reporte para su posterior estudio.
- **Ayuda:** El módulo ayuda contiene información sobre el desarrollo del proyecto, archivos de ayuda para el usuario sobre el uso del software (manual de usuario) e información de la ISO/IEC 27001 junto con enlaces para profundización sobre el tema.

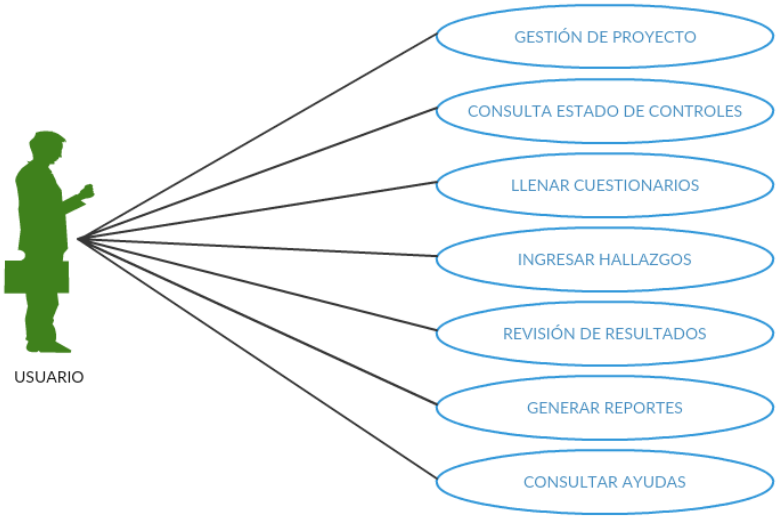
5.2.1.3. Requerimientos no funcionales

- **Desempeño:** La aplicación no cuenta con elementos que entorpezcan su rendimiento y podrá funcionar en equipos de gama baja con eficiencia en su uso.
- **Seguridad:** Las credenciales permiten que la administración de la información contenida solo sea de conocimiento de los usuarios responsables.
- **Integridad:** El sistema, bajo el uso normal de sus características y en cumplimiento de sus requerimientos normales de instalación funcionará sin problemas, en caso de presentarse errores el usuario deberá remitirse a los manuales de usuario o sistema.
- **Disponibilidad:** La eficiencia sumada a la seguridad permiten obtener de forma inmediata los datos de los proyectos que se gestionen.
- **Interfaz sencilla:** El aplicativo es estándar a cualquier aplicación y puede ser usada por cualquier persona con experiencia básica en el uso de software.
- **Portabilidad:** El software puede ser usado en un sistema operativo compatible que tenga la máquina virtual de JAVA y cuyo hardware cumpla con requerimientos mínimos de rendimiento.

5.2.2. DISEÑO ORIENTADO A OBJETOS

5.2.2.1. Diagramas de casos de uso

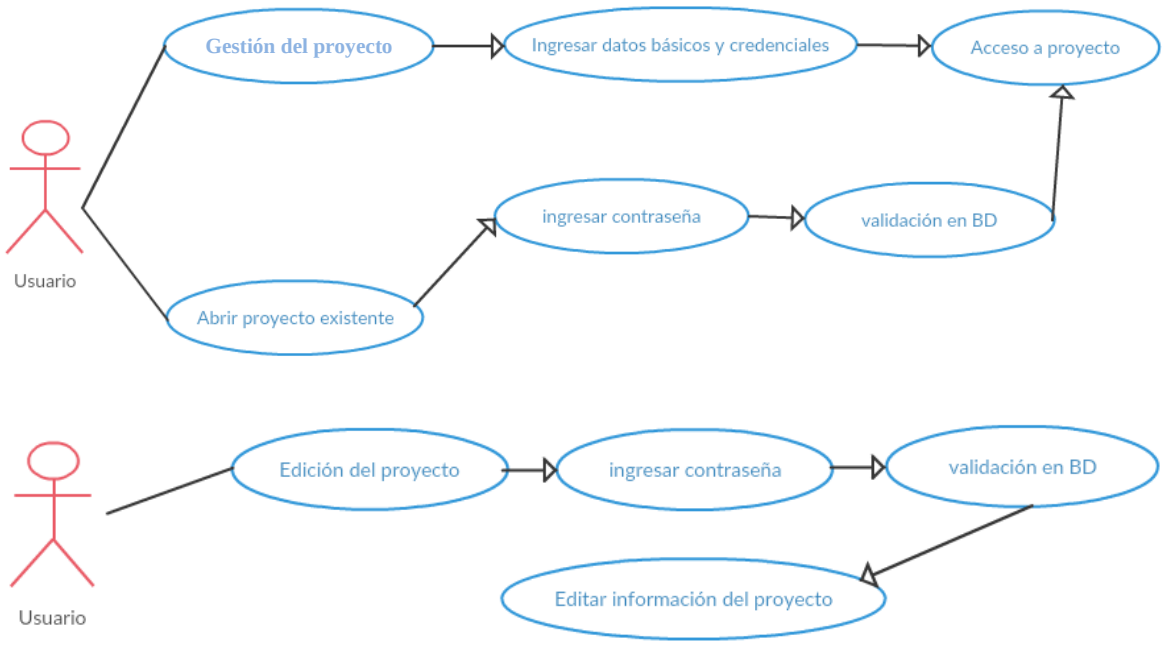
Caso de uso 1: Tareas principales del usuario



ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Gestión de proyecto**	Luego de iniciar la aplicación la primera vez el usuario deberá crear un nuevo proyecto, ingresar datos del mismo y las credenciales de validación, luego el usuario podrá iniciar sesión en un proyecto creado en las siguientes ejecuciones o crear nuevos.
	Consulta de controles	El usuario puede ver el listado de controles donde se indica también las estadísticas de avances del proyecto y a partir de aquí podrá consultar los cuestionarios.
	Llenar cuestionarios	Cuestionarios correspondientes con cada control de la norma ISO 27001 de 2013, su diligenciamiento permite generar los resultados.
	Ingresar hallazgos	Además de los campos de los cuestionarios existe un espacio donde se podrá guardar una descripción de hallazgos, esto no afecta los resultados.
	Revisión de resultados	El usuario puede consultar los resultados de los avances en la solución de cuestionarios con el fin de que pueda ver los puntos fuertes y débiles además de lo que está pendiente por revisar.
	Generar reportes	Los resultados se observan en el software, pero los mismos pueden ser exportados en forma de

		reportes a archivos de distinto formato para ser presentados o consultados.
	Consultar ayudas	En este apartado el usuario puede consultar los documentos de ayuda dirigidos a guiar tanto en el manejo adecuado del software como a datos sobre la norma ISO 27001 que facilitan la comprensión y diligenciamiento de cuestionarios.

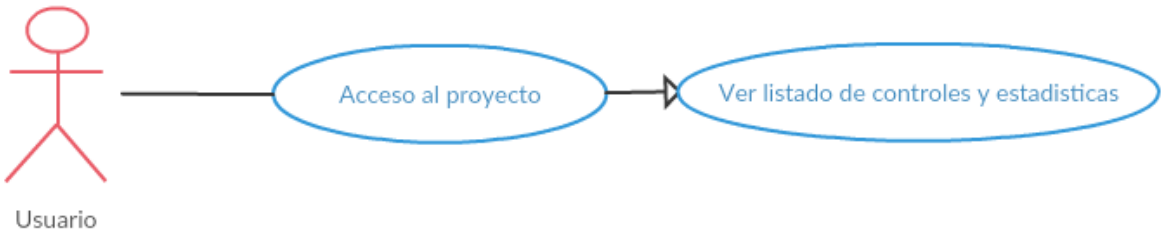
Caso de uso 2: Gestión de proyecto



ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Ingresar datos básicos y credenciales**	Para la creación de un nuevo proyecto es necesario ingresar datos de identificación como nombre de la organización y descripción del proyecto además de una contraseña de seguridad.
	Acceder al proyecto	Se accede al proyecto inmediatamente luego de su creación, se accede a un proyecto existente por medio de su contraseña.
	Abrir proyecto existente	Al ejecutar el software el usuario puede escoger ingresar a un proyecto ya creado.
	Ingresar contraseña	Cada proyecto está protegido por contraseña digitada por el usuario para protegerla de posibles cambios indebidos por terceros.
	Validación en base de datos	El software realiza una conexión con BD verificando que la contraseña coincida con el proyecto en cuestión.

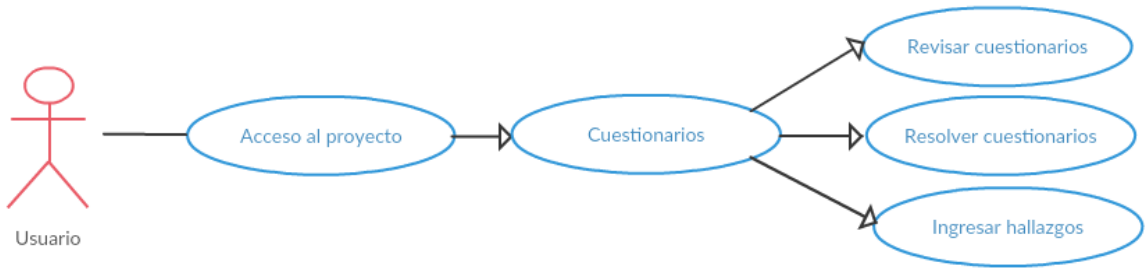
	Edición del proyecto	El usuario puede cambiar la información de un proyecto existente una vez que haya ingresado en el mismo, sin embargo por razones de seguridad se solicitará nuevamente la contraseña

Caso de uso 3: Consulta de estado de controles



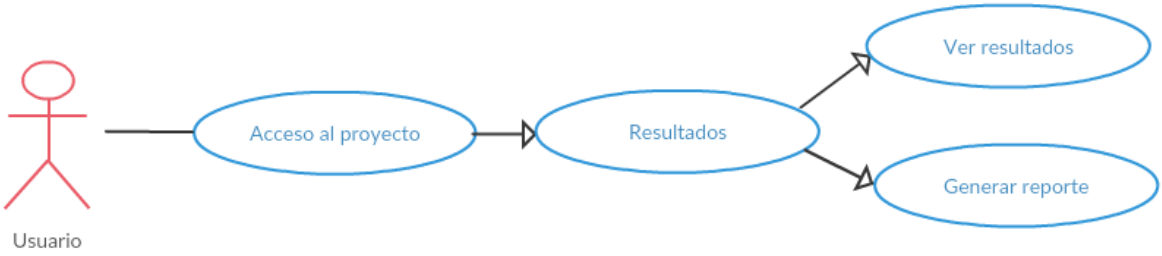
ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Acceder al proyecto**	Se puede consultar controles una vez se ha escogido un proyecto
	Ver listado de controles y estadísticas	El proyecto mostrara en primer lugar, además de los datos básicos del mismo un resumen estadístico sobre los avances en el desarrollo de cuestionarios y el listado de cuestionarios con su respectivo nivel de cumplimiento.

Caso de uso 4: Cuestionarios



ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Acceder al proyecto**	Se puede consultar controles una vez se ha escogido un proyecto
	Cuestionario	Entre las opciones del proyecto se permite ingresar a los cuestionarios a partir de la lista de controles.
	Revisar cuestionarios	Al ingresar en uno de los controles se puede ver el estado de los cuestionarios, correspondiente con los valores con los que fue diligenciado
	Resolver cuestionarios	El usuario podrá resolver un cuestionario que no ha sido diligenciado o editar los valores de cualquier cuestionario.
	Ingresar hallazgos	Además de resolver los formularios el usuario puede ingresar la descripción de los hallazgos en campos de texto de cada formulario los cuales corresponderán con los controles de la norma y servirán de referencia al usuario.

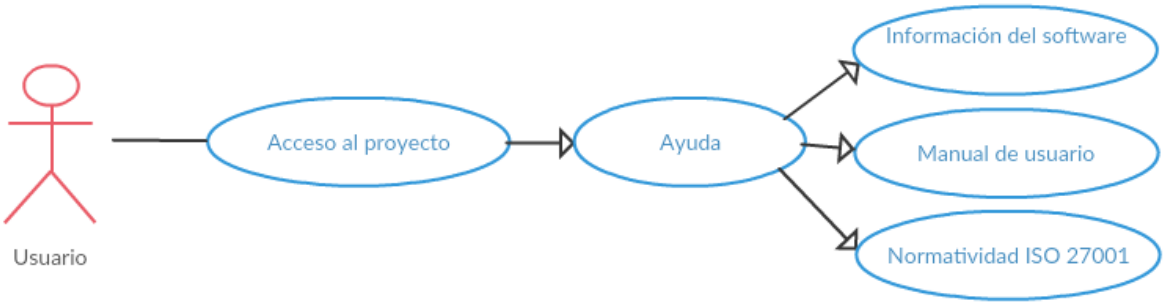
Caso de uso 5: Revisión de resultados y generador de reportes



ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Acceder al proyecto**	Se puede consultar resultados dentro de un proyecto
	Resultados	El menú Resultados permite escoger la forma como serán visualizados dichos resultados.
	Ver resultados	El usuario tendrá una vista de los resultados

		parciales o totales según lo desee sobre los avances alcanzados en la solución de formularios.
	Generar reporte	De la misma forma que la vista previa de resultados, el generador de informes permite escoger el tipo de informe que se desea y posteriormente escoger el tipo de salida que se obtendrá como archivo externo.

Caso de uso 6: Ayuda



ACTOR	CASO DE USO	DESCRIPCION
USUARIO	**Acceder al proyecto**	Se puede consultar resultados dentro de un proyecto
	Ayuda	El módulo de ayuda da acceso a archivos de ayuda e información relevante al software y su uso.

5.2.2.2. Diagramas de secuencia

Diagrama 1: Creación de proyecto

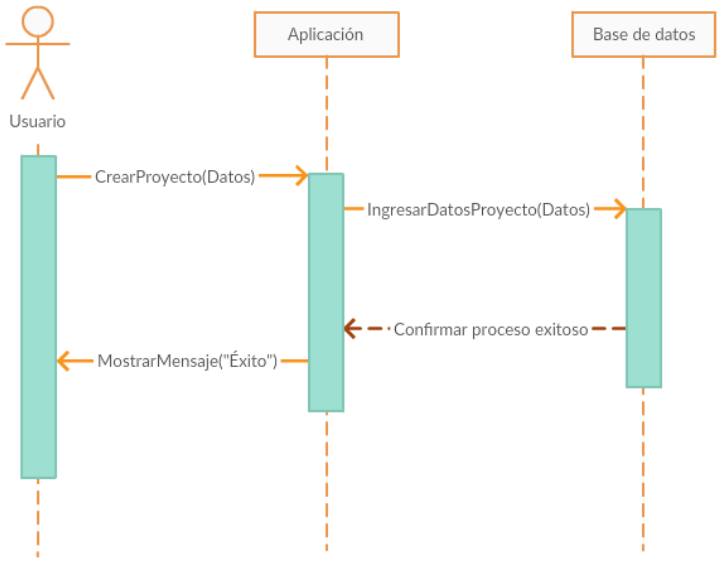


Diagrama 2: Acceso a proyecto existente

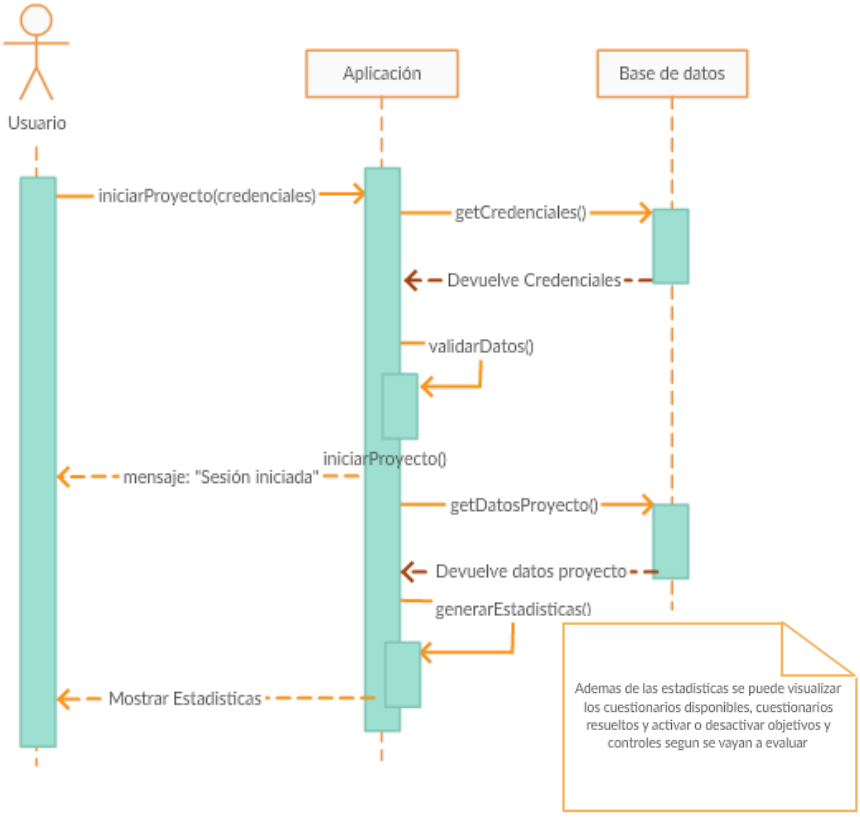


Diagrama 3: Resolver cuestionario

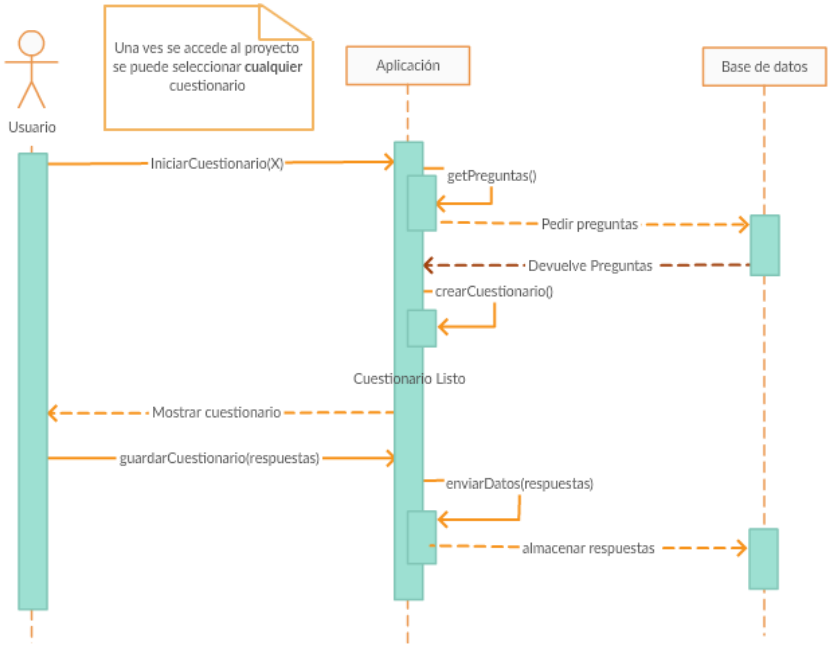
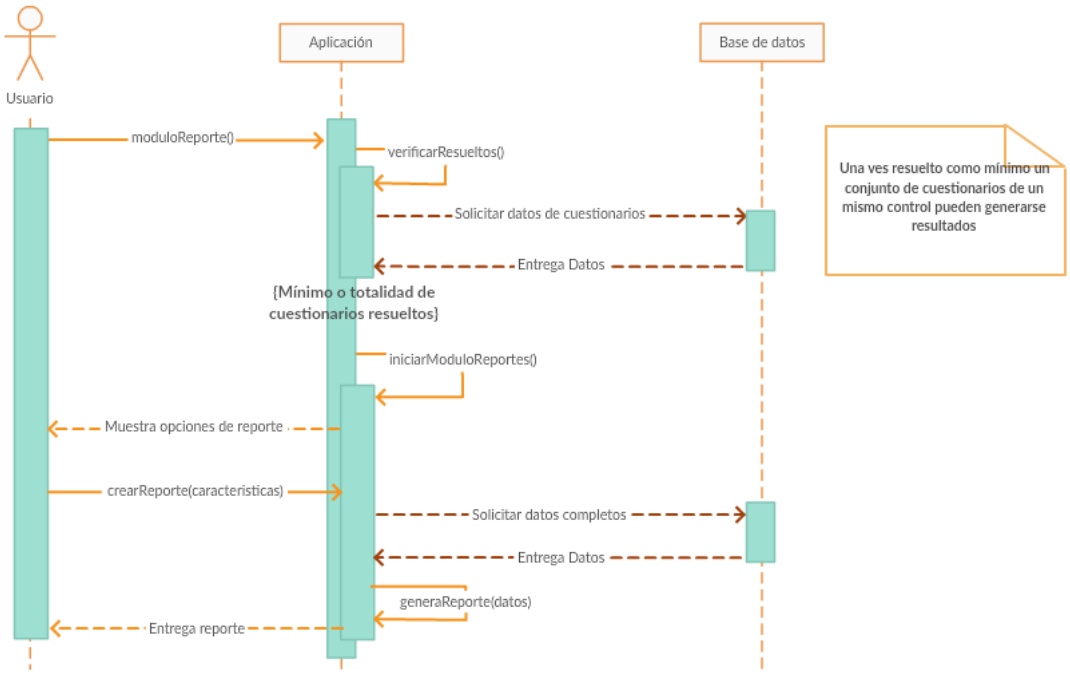


Diagrama 4: Generar reporte



5.2.3. MAPA FUNCIONAL DEL SOFTWARE

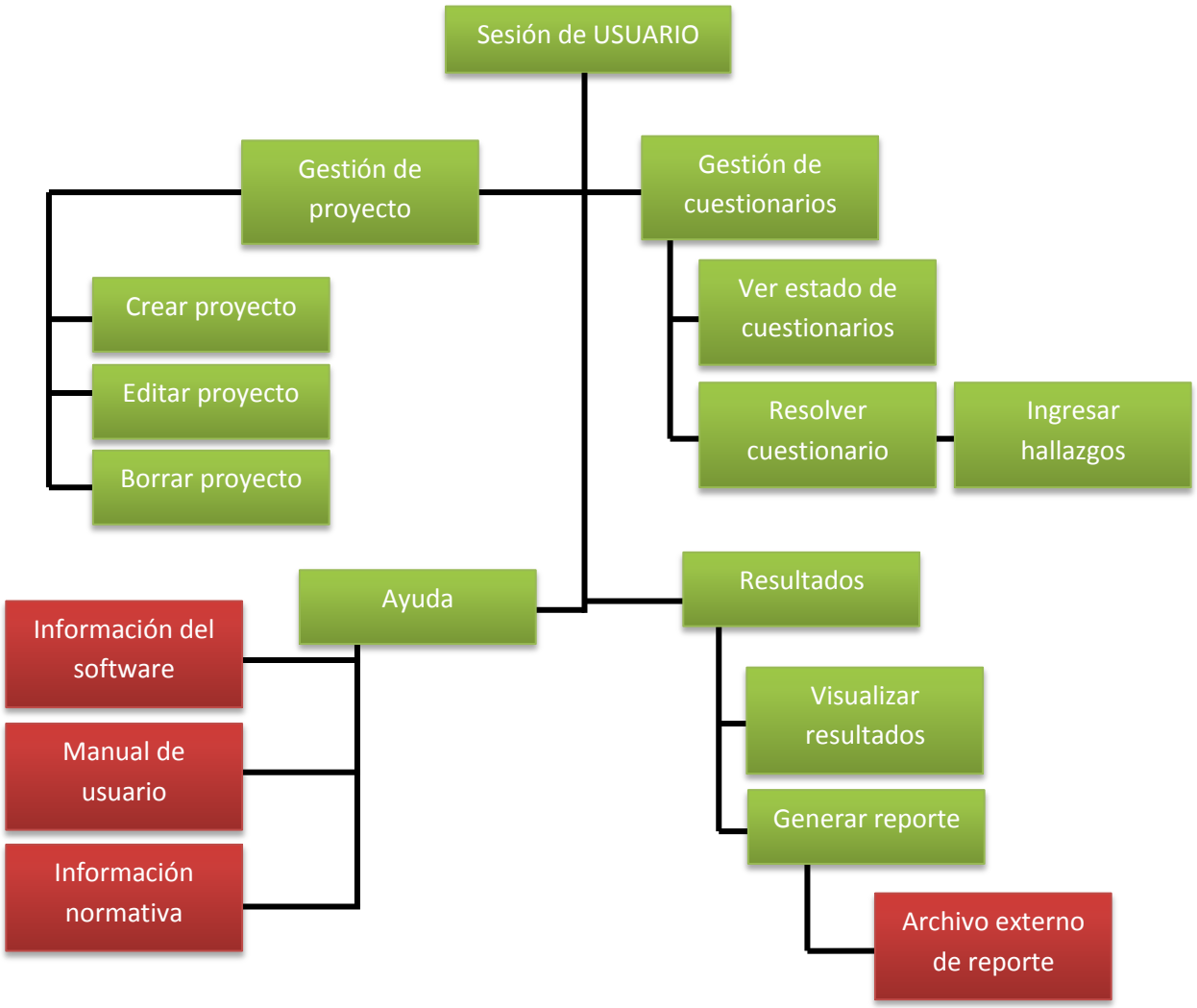
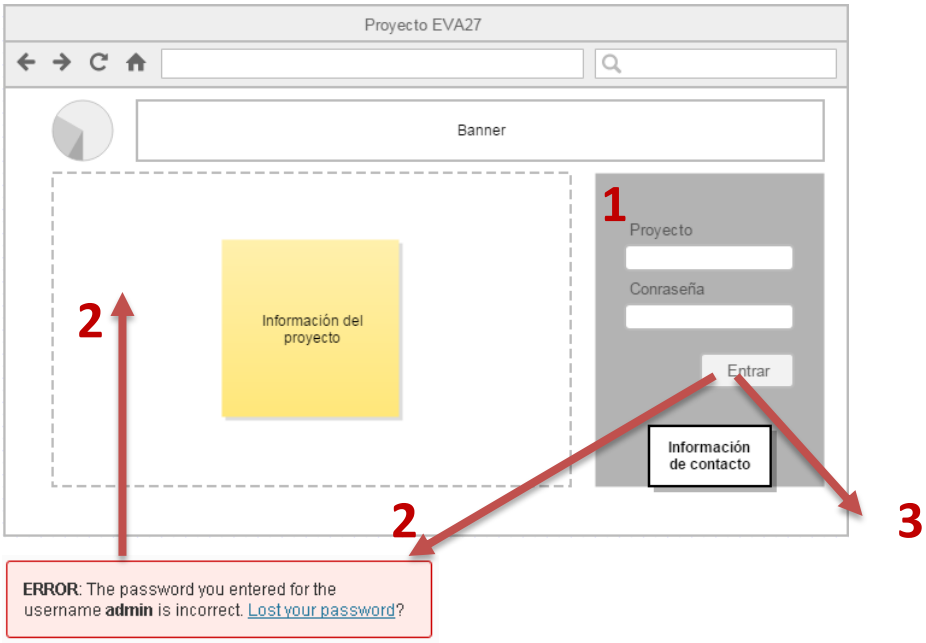


Ilustración 8: Mapa funcional del software

5.2.4. DISEÑO DE LA INTERFAZ DE USUARIO

Interfaz 1: Inicio de la aplicación y formulario de ingreso

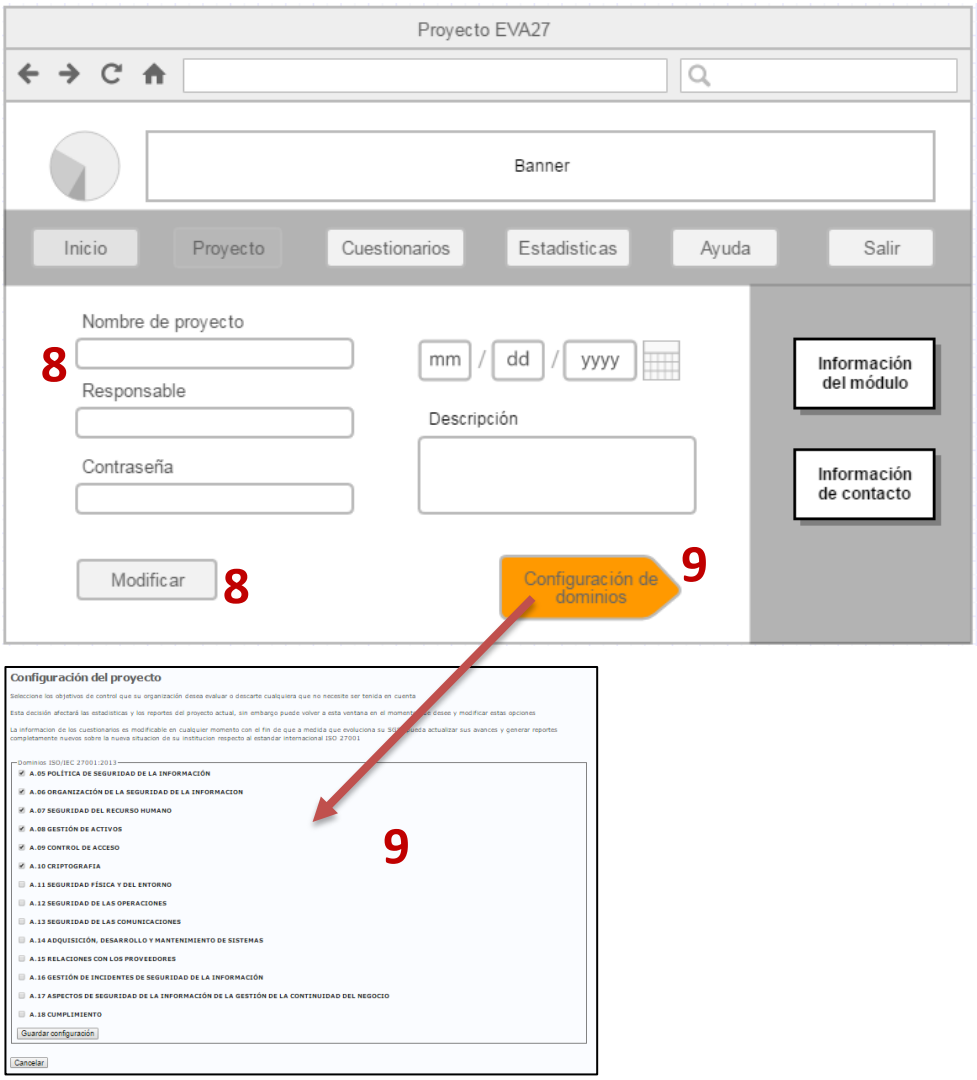


1. El inicio de sesión se realizará por medio del ingreso del nombre del proyecto y la contraseña del mismo los cuales serán asignados directamente a la base de datos.
2. En caso de que el inicio de sesión sea insatisfactorio se genera una ventana de información el sistema no pasará de la primera interfaz
3. En caso de que el inicio sea satisfactorio se ingresa en la interfaz 2.

Interfaz 2: Página de inicio

4. Una vez iniciado sesión se observará en la parte superior el menú que permitirá acceder a los distintos módulos del proyecto.
5. Se reservará un área en el lado izquierdo que dependiendo del módulo actual puede cumplir distintas funciones
6. En este módulo se presentará información del proyecto y el mapa del sitio.
7. El botón salir del menú, en cualquier momento del proyecto permitirá cerrar sesión de forma segura y volver a la primera interfaz

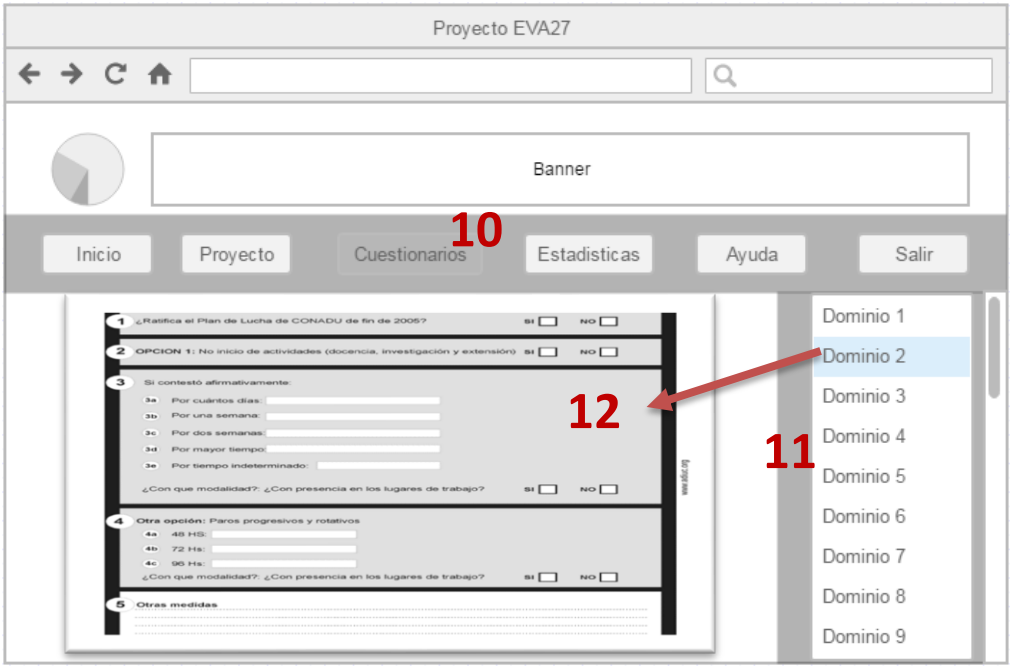
Interfaz 3: Módulo Proyecto



8. El módulo proyecto mostrará la información del proyecto que fueran suministrados por el usuario o creadores del mismo, dichos datos podrán ser modificados desde este módulo a través del botón “Modificar”.
9. El botón “Configuración de dominios” es uno de los más importantes para los usuarios del proyecto quienes podrán, a través de una ventana, determinar cuáles dominios realmente pueden ser tenidos en cuenta dentro del proyecto, toda la

información de cuestionarios, estadísticas o resultados será únicamente obtenida de los dominios activos.

Interfaz 4: Módulo Cuestionarios

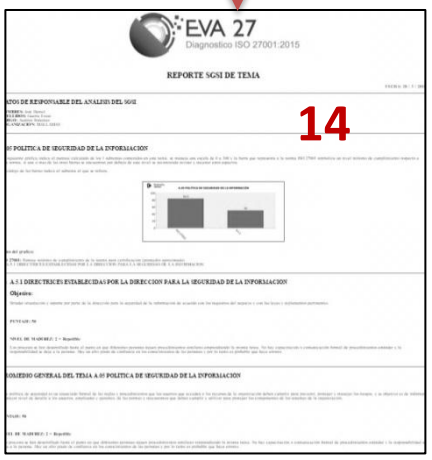


10. El módulo cuestionarios permite al usuario resolver los cuestionarios de control que, basado en la norma ISO 27002 muestra las recomendaciones que lograrán medir cada control de cada objetivo, de cada dominio.

11. En el menú lateral se mostrara el listado de dominios y objetivos de control.

12. Al seleccionar un objetivo de control se podrá escoger un cuestionario de control para ser resuelto

Interfaz 5: Estadísticas del proyecto



13. El módulo de estadísticas mostrará una visión general del proyecto, mostrando avances en el desarrollo del mismo y el estado de seguridad de cada dominio hasta el momento, esta información se podrá ampliar en los reportes.

14. El botón reportes permite abrir una ventana donde se escogerá el tipo de reporte que será creado, desde una visión general del proyecto que amplía la información de estadísticas hasta reportes más específicos sobre un determinado dominio u objetivo de control, con la condición de que se encuentre debidamente diligenciado.

5.2.5. DISEÑO DE BASE DE DATOS

Para la creación de la base de datos se tiene en cuenta la división de los cuestionarios que van acorde con la distribución de los controles de la norma ISO 27001, esta división comienza de la siguiente forma: en primer lugar están los Objetivos de control (Tema) con su respectiva descripción, estos abarcan los Controles (Subtema) los cuales tienen sus respectivos objetivos de cumplimiento, cada uno de ellos correspondientes con los cuestionarios que cuentan con una guía de implementación y los puntos a resolver además del campo donde serán registrados los hallazgos.

Finalmente la parte central de la herramienta son las valoraciones o respuestas a las que se enlaza el proyecto, Optando por un diseño lo más sobrio posible para obtener la mayor eficiencia se tiene las siguientes tablas:

- Tema
- Subtema
- Cuestionario
- Pregunta
- Hallazgo
- Respuesta
- Proyecto
- Valor

DIAGRAMA 1: Modelo entidad relación

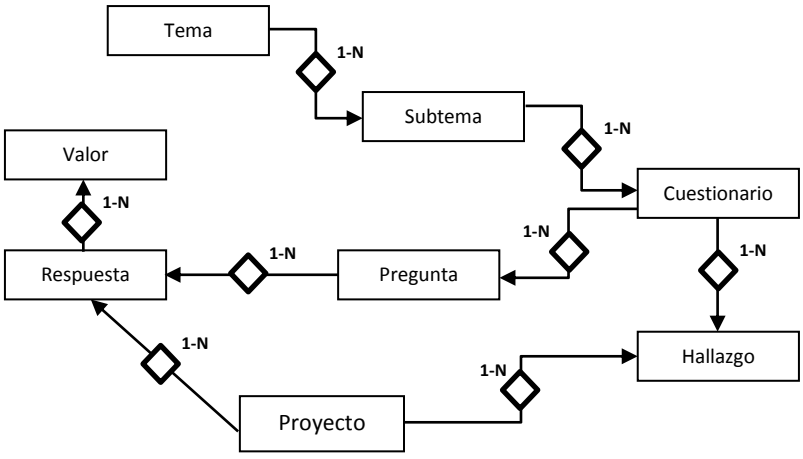


DIAGRAMA 2: Esquema relacional

TEMA		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_tem	int(5)	not null
nom_tem	varchar(100)	not null
des_tem	text	not null

SUBTEMA		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_stm	int(5)	not null
nom_stm	varchar(100)	not null
obj_stm	text	not null
cod_tem	int(5)	not null

CUESTIONARIO		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_tem	int(5)	not null
nom_cue	varchar(100)	not null
ctr_cue	text	not null
gui_cue	text	not null
cod_stm	int(5)	not null
tip_dis	bit(1)	not null
tip_evi	bit(1)	not null
tip_pre	bit(1)	not null
tip_dtc	bit(1)	not null
tip_rea	bit(1)	not null
tip_rec	bit(1)	not null
obj_con	bit(1)	not null
obj_int	bit(1)	not null
obj_dis	bit(1)	not null

PREGUNTA		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_pre	int(5)	not null
nom_pre	text	not null
cod_cue	int(5)	not null

RESPUESTA		
Nombre	**Tipo (Longitud)**	**Nulos**

cod_res	int(6)	not null
cod_mmz	int(1)	not null
cod_pre	int(5)	not null
ide_pro	int(5)	not null

VALOR		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_mmz	int(1)	not null
nom_mmz	varchar(20)	not null
des_mmz	text	not null

HALLAZGO		
Nombre	**Tipo (Longitud)**	**Nulos**
cod_hal	int(6)	not null
des_hal	text	not null
cod_cue	int(5)	not null
cod_pro	int(6)	not null

PROYECTO		
Nombre	**Tipo (Longitud)**	**Nulos**
ide_pro	int(6)	not null
nom_pro	varchar(50)	not null
org_pro	varchar(50)	not null
deo_pro	varchar(50)	not null
pwr_pro	varchar(30)	not null

6. CAPITULO 6: DESARROLLO

Muchas de las organizaciones que anteriormente usaban clientes instalables están convirtiéndose a un entorno web pensando principalmente en las enormes ventajas de centralización, actualización y acceso fácil desde cualquier dispositivo.

Teniendo en cuenta esta tendencia además de las ventajas nombradas en el marco referencial (**3.2.9 Aplicaciones web y aplicaciones de escritorio**) se ha desarrollado esta aplicación en lenguajes web, específicamente PHP, HTML5, Javascript y con un motor de base de datos en MySQL, estas son todas opciones muy básicas pero al mismo tiempo muy usadas por lo que tienen una gran compatibilidad y gran capacidad de evolucionar de acuerdo con la intención académica del proyecto además de ser gratuitas.

El motor de base de datos de MySQL ofrece bastantes ventajas además de su gratuidad, principalmente la velocidad y la fiabilidad además de la integración que tiene con el lenguaje PHP crean entre ellos un entorno dinámico de desarrollo rápido que se adapta al modelo de desarrollo establecido para este proyecto **Prototipos Incrementales (ver 3.2.7)**.

En general se trata de un sistema desarrollado bajo el enfoque funcional con un diseño lo más liviano posible para dar resultados de forma eficiente.

Siguiendo con el diseño propuesto se desarrollaron las siguientes funciones:

6.1. MÓDULO PROYECTO

Los usuarios de cada proyecto tendrán una cuenta del mismo donde podrían aprovechar las funcionalidades del programa de forma individual. Por seguridad, no se contaría con un medio para inscribirse a la herramienta a través de la página de entrada (como se puede observar en las páginas de correo electrónico o foros gratuitos) sino que estos tendrían que comunicarse con el desarrollador (o administrador de la herramienta) para obtener de forma gratuita un permiso de uso de la misma.

La información básica de cada proyecto se ingresará directamente en la base de datos. Una vez hecho esto se enviaría los datos de ingreso al usuario para que empiece a hacer uso de la herramienta. El usuario ingresa con un Nick (según el nombre del proyecto) y una contraseña, luego dentro de la herramienta con todos los botones activos para acceder a cualquier función también podría acceder a la pestaña correspondiente al proyecto donde encontraría todos los datos que podrán ser modificados en cualquier momento, esto no afectará los resultados de la evaluación pero si aparecerá en los reportes.

Sobre el orden del menú, aunque obedecía inicialmente la metodología para la evaluación de SGSI se tuvo en cuenta la comodidad del usuario, ya que la información del proyecto no sería continuamente editada, por este motivo se envía al final esta opción.

6.2. MÓDULO ESTADISTICAS

El módulo estadísticas consiste en un espacio informativo general del proyecto que ayudará al usuario auditor a revisar los avances en el diligenciamiento de los cuestionarios y el estado general del proyecto, entre otros muestra la siguiente información:

- ✓ Cuestionarios pendientes y resueltos.
- ✓ Cantidad de Hallazgos
- ✓ Nivel porcentual actual de cada objetivo de calidad de la información por cada dominio.
- ✓ Valor de cumplimiento general de las características Disuasión, Evasión, Prevención, Detección, Reacción, Recuperación.

6.3. MODULO CUESTIONARIOS

Este es el módulo más importante en cuanto a la investigación y al objetivo de la herramienta software. Por la cantidad de cuestionarios se pensó que tomaría mucho tiempo generar uno por uno, sin embargo haciendo un análisis y teniendo en cuenta las herramientas que ofrece el lenguaje de programación PHP con asociación a una base de datos se pudo concluir que se podía traer los cuestionarios desde esa misma base de datos a un solo cuestionario que cambiaría de datos dependiendo del tema - subtema escogido.

De acuerdo con el diseño propuesto se genera un menú en el lado derecho que muestra los dominios, al escoger uno se desplegaran los objetivos de control y al hacer clic en cualquiera de ellos cambiará el panel principal de la herramienta, dando una descripción del objetivo de control y listando los cuestionarios de control.

Al seleccionar un cuestionario de control se abre una ventana con dicho cuestionario y toda la información adicional (controles y guías de implementación) desde la base de datos. Frente a cada recomendación se

pone una caja de selección donde el usuario auditor deberá escoger el nivel de madurez de cada acción recomendada para el cumplimiento del control.

Es importante recordar que este consiste en 6 niveles o calificaciones posibles a cada recomendación que son: INEXISTENTE, INICIAL, REPETIBLE, DEFINIDO, ADMINISTRADO, OPTIMIZABLE. Finalmente cuando se respondiera a un cuestionario se requería que las respuestas fueran guardadas en la base de datos y que estas respuestas siguieran disponibles o seleccionadas cuando se consultará nuevamente el mismo cuestionario, el modo como las respuestas de cada usuario entran a la base de datos es uno de los más importantes ejemplos de asociación de los módulos: para las respuestas era necesario saber a qué pregunta se respondía, era necesario saber que usuario estaba respondiendo a dicha pregunta y era necesario saber qué respuesta se había dado a esta pregunta. Este es el corazón de la base de datos, donde converge la información para que la herramienta tenga un sentido y se puedan generar unas salidas. Es importante aclarar que la información o las respuestas registradas de cada cuestionario son modificables. En cada auditoria se define los puntos que requieren de unas correcciones y se avanza en cuanto a mejorar o reparar estos puntos, estas respuestas son modificables porque se pensó en que se debían poder variar dependiendo de los avances que tenga un SGSI en el transcurso del tiempo para generar unas salidas diferentes.

Así mismo cada cuestionario de control cuenta con el espacio donde se podrán guardar, editar o eliminar los hallazgos. La evaluación de las características de seguridad y objetivos de calidad del control son intrínsecas, es decir, cada control ya tiene su clasificación y el valor que se dará a cada una corresponderá con la evaluación del control.

6.4. MODULO REPORTES

Es el módulo desde donde se puede generar las salidas del programa, después de que el usuario ha hecho uso de la herramienta y he respondido completamente a un **Objetivo de control** o **Dominio** o a la totalidad de los cuestionarios. En principio al ingresar a este módulo se encontrara un espacio informativo en donde se muestran todos los Dominios, Objetivos de control y Controles mostrando su estado por medio de dos símbolos con la finalidad de que el usuario sepa identificar cuáles han sido resueltos y cuales están pendientes.

La segunda parte de la herramienta consiste en un **ASISTENTE DE REPORTES** que se ejecuta en una ventana aparte de la misma forma que los cuestionarios y desde donde se puede elegir el tipo de reporte que

puede ser REPORTE GENERAL (todos los cuestionarios de control activos deben estar respondidos, se busca la calificación final), REPORTE DE DOMINIO (todos los Objetivos de control correspondientes deben estar respondidos y es un poco más específico ya que describe el estado del dominio y sus objetivos de control), REPORTE DE OBJETIVO (todos los cuestionarios de control correspondientes deben estar respondidos, es el reporte más específico ya que muestra el nivel de madurez de cada control).

Este módulo de salidas se pensó como un reporte bastante sencillo y sobrio, que mostrará la información más relevante, de manera que permita anexarse a un documento más completo de un reporte de auditoría. En estos reportes también se puede encontrar la gráfica que ayuda a comprender más fácilmente el estado de los ítems (generales o específicos) del SGSI y compararlo con la norma ISO 27001.

6.5. BOTON AYUDA

Consiste simplemente en el manual del usuario en formato PDF donde se compila toda la información referente al funcionamiento de la herramienta.

La información sobre como el usuario debe operar frente a la interfaz de cada uno de los módulos anteriormente expuesto, se podrá en encontrar en el ANEXO 1: MANUAL DE USUARIO.

7. CAPITULO 7: VALIDACIÓN Y PRUEBAS

Uno de los retos en la realización de una aplicación de este estilo tiene que ver con el apoyo de organizaciones que estén dispuestas a prestar su información y revelar hasta cierto punto el estado de su nivel de seguridad.

Esto fue especialmente difícil y se llegó a la conclusión de que no se podrían obtener datos demasiado específicos que pusieran en riesgo la seguridad de la información.

Las organizaciones listadas a continuación prestaron su información a través de las personas que se nombra en cada caso quienes son encargados del área correspondiente o tienen el conocimiento suficiente para dar respuesta a los cuestionarios.

7.1. ORGANIZACIÓN 1: Fundación de servicios educativos de EMSSANAR - CETEM

MISIÓN: Es un Centro de estudios comprometido con la formación para el trabajo y el desarrollo humano, que se rige por los principios de solidaridad, liderazgo, y responsabilidad social, brindando servicios educativos en las áreas de: sistemas, financieras y de salud que contribuyan a la formación integral de jóvenes y adultos del departamento de Nariño, con espíritu emprendedor, crítico y solidario. Contamos con un talento humano comprometido, cualificado y una infraestructura física y tecnológica acorde a las áreas de formación establecidas. Nuestro campo de acción se centra en la formación por competencias de conformidad a las exigencias del sector productivo y a la normatividad vigente del sistema educativo Colombiano.

VISIÓN: En año 2.019 seremos un Centro de Estudios de la economía solidaria, reconocido por su aporte a la generación de capital social y desarrollo sostenible.

OBJETIVO: Contribuir a la generación de capital social y desarrollo socioeconómico de la región, a través de procesos pertinentes de educación técnica laboral bajo el modelo de competencias que permitan la vinculación del egresado al sector productivo.

USUARIO APLICATIVO: Ing. Armando Coral, Coordinador del área informática

7.2. ORGANIZACIÓN 1: INSTITUCIÓN UNIVERSITARIA CESMAG. (Facultad Ingeniería)

MISIÓN: La Institución Universitaria Centro de Estudios Superiores María Goretti es una entidad Católica, de carácter privado, orientada por los principios franciscano-capuchinos y la filosofía personalizante y humanizadora de su fundador, padre Guillermo de Castellana; promueve la formación integral de profesionales con espíritu crítico, ético y reflexivo, capaces de comprender y solucionar problemas desde su campo de acción profesional con perspectiva global, a través de la docencia, la investigación e innovación y la extensión.

VISIÓN: En el año 2019, la Institución Universitaria Centro de Estudios Superiores María Goretti será reconocida como universidad por su calidad académica, desarrollo investigativo y de innovación, servicio a la sociedad y condiciones organizacionales adecuadas, para contribuir al desarrollo sostenible a nivel regional y nacional, con perspectiva internacional.

USUARIO APLICATIVO: Ing. Luis Carlos Revelo,

7.3. ORGANIZACIÓN 1: EPS Indígena MALLAMAS

MISIÓN: "MALLAMAS EPS-INDIGENA es una Entidad de Derecho Público de Carácter Especial que garantiza el aseguramiento en salud, a la población indígena y no indígena del territorio Colombiano, enfocado en generar condiciones que protejan la salud de la población afiliada, a través de procesos transparentes, eficientes y oportunos, protegiendo y garantizando de manera efectiva los derechos a la Seguridad Social en Salud promoviendo el respeto a su estilo de vida, su integridad étnica, sus creencias y sus valores socioculturales.".

VISION: "Seremos en el año 2017 una entidad altamente competitiva, responsable y reconocida como líder en el aseguramiento en salud en el territorio nacional, logrando generar condiciones que protejan la salud de la población afiliada, basados en la cultura de autocontrol, en el mejoramiento

permanente de nuestros procesos y en el desarrollo eficiente del talento humano y tecnológico; respetando y apoyando el saber ancestral y las particularidades étnoculturales.".

OBJETIVO: Garantizar la prestación de los servicios de aseguramiento en salud, brindando a sus afiliados: Facilidad de acceso a los servicios, una red idónea y suficiente, que permita la prestación oportuna y segura de los servicios de salud; apoyado en el respeto por la cultura, la participación proactiva de la comunidad indígena y no Indígena, en el permanente desarrollo del Talento Humano, en el manejo adecuado de los recursos y en un eficiente sistema de Información. Estamos convencidos que el mejoramiento continuo de los procesos nos permitirá lograr la satisfacción de los afiliados de MALLAMAS EPS-I y por ende optimizar su calidad de vida."

USUARIO APLICATIVO: Ing. Jorge Daniel Carlderon, Coordinador del área informática

El enlace al aplicativo fue enviado a cada uno de los responsables junto con una encuesta sobre la funcionalidad del sistema (ver Anexo 3) y los resultados obtenidos pueden verificarse en los anexos 4, 5 y 6 respectivos a cada una de las organizaciones anteriormente nombradas

8. CAPITULO 8: DISCUSIÓN Y ANÁLISIS DE RESULTADOS

En distintos foros, textos, discusiones de todo tipo y blogs sobre seguridad de la información donde se aborde el tema de la auditoría y la certificación a través de ISO/IEC 27001 (desde la versión 2005 hasta la revisión actual) siempre se está de acuerdo en una afirmación:

“No existe una forma fácil, resumida o un camino corto para efectuar el proceso de auditoría”

Es una afirmación dura para la ejecución de un proyecto como el presente pero también abre otros caminos sobre las distintas formas en que se puede prestar ayuda en el desarrollo de este complejo proceso.

La única forma de efectuar un estudio que entregue unos resultados claros y completos que llenen las expectativas de una auditoría era por medio de un estudio a fondo de cada tema de la seguridad de la información; el problema era que no se podía generar en si una herramienta que pudiera hacer ese estudio ya que se trataba de demasiados aspectos, muchos de ellos humanos, que además demanda muchos permisos, tiempo y experiencia por parte de los involucrados.

¿Pero qué pasa si se desea obtener un punto de partida, una valoración inicial sobre el estado del SGSI pero que involucre además los dominios, objetivos de control y controles de la norma ISO 27001 y 27002?

Esto es posible de lograr si se aborda la norma ISO 27002:2015, en ella hay un conjunto de recomendaciones para lograr el cumplimiento de cada control de la norma ISO/IEC 27001 de 2013. Este enfoque si esta propuesto en muchos de los sitios nombrados donde se habla sobre el tema de SGSI y se ve la necesidad de proponer una herramienta completa pero sencilla y fácil de usar que pueda llenar este vacío inicial del proceso de auditoría.

El programa entonces responde a esta necesidad ya que por medio de los resultados de sus cuestionarios mide el nivel de cada dominio teniendo en cuenta el modelo de madurez propuesto por COBIT para poder así clasificar el nivel de madurez en que se encuentra cada control, cada objetivo de control y cada dominio de seguridad planteado en la norma ISO 27001 de 2013.

Para probar la utilidad de este software se solicitó a personal de la coordinación de sistemas de distintas organizaciones para que probaran y respondieran a los diferentes cuestionarios basados en su conocimiento del área de la seguridad, su experiencia y su observación, es decir que simplemente se llevó a cabo una prueba informal para determinar un nivel de seguridad de la información aproximado de cada una de estas dos organizaciones.

Las organizaciones estudiadas fueron la EPS I MALLAMAS, la Institución universitaria CESMAG y el centro de estudios técnicos de Emssanar CETEM, después de que hizo uso de la herramienta y se respondieron completamente a todos los cuestionarios se ejecutó el reporte general de cada una dando como salida una calificación final de seguridad que además es comparada con un mínimo de cumplimiento de la norma ISO 27001 para determinar si la organización puede pensar seriamente en una certificación bajo dicha norma.

Los resultados se resumen en las siguientes tablas:

	Puntaje General		
Dominios \ Organización	**IU. CESMAG**	**EPSI MALLAMAS**	**EMSSANAR CETEM**
A.5 Políticas de Seguridad	65.31	72.08	
A.6 Organización de la seguridad de la información	59.7	60.22	61.9
A.7 Seguridad en recursos humanos			52.93
A.8 Administración de activos	60.67	56.54	49.2
A.9 Control de acceso	64.21	50.86	59.55
A.10 Criptografía	49	59.5	
A.11 Seguridad física y ambiental	62.49	71.69	57.18
A.12 Seguridad en operaciones	59.1	57.96	56.66
A.13 Seguridad en comunicaciones	62.23		67.37
A.14 Adquisición, desarrollo y mantenimiento de sistemas	63.7	57.86	
A.15 Relación con proveedores		41.25	
A.16 Administración de incidentes de seguridad de la información	58.33	41.29	
A.17 Aspectos de seguridad de la información en la administración de continuidad del negocio	62.08	55.6	24.05
A.18 Cumplimiento	60.19	65.26	49.11
PROMEDIO GENERAL:	**60.58**	**57.51**	**53.11**

Las organizaciones anteriormente estudiadas son de diferente naturaleza y tamaño, características que afectan el resultado final, esto también influye en los dominios que se desactivaron, los responsables manifestaron o no tener conocimiento suficiente sobre el área del dominio o que la organización no profundizaba lo suficiente en controles de seguridad sobre esos temas.

IU CESMAG: Según los resultados obtenidos se puede decir que el nivel de madurez general de la organización es el nivel DEFINIDO, es decir que, aunque no alcanzan un nivel certificable se trata de un nivel de madurez lo suficientemente organizado en cuanto a la protección de su información, la definición del nivel definido es la siguiente: “los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.”

EPS-I MALLAMAS: Según los resultados obtenidos se puede decir que el nivel de madurez general de la organización es el nivel DEFINIDO, es decir que, aunque no alcanzan un nivel certificable se trata de un nivel de madurez lo suficientemente organizado en cuanto a la protección de su información, la definición del nivel definido es la siguiente: “los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.”

Emssanar CETEM: Según los resultados obtenidos se puede decir que el nivel de madurez general de la organización es el nivel DEFINIDO, es decir que, aunque no alcanzan un nivel certificable se trata de un nivel de madurez lo suficientemente organizado en cuanto a la protección de su información, la definición del nivel definido es la siguiente: “los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.”

El puntaje mínimo necesario para que una organización pueda certificarse bajo la norma ISO/IEC 27001 debe ser igual o mayor a 83.5 en donde el nivel de madurez es ADMINISTRADO. Esto nos puede ayudar a concluir que el estado de los sistemas de gestión de seguridad de la información (SGSI) en las organizaciones estudiadas aun no cumplen con los requerimientos mínimos establecidos en la norma ISO/IEC 27001:2005.

Esta conclusión puede ser de gran valor para una organización la cual puede identificar fácilmente su punto de partida, los eslabones más débiles a trabajar para lograr la certificación o por lo menos un nivel aceptable de seguridad.

9. CONCLUSIONES

- Del presente proyecto se concluye que la información que se encontró asociada con sistemas de gestión de seguridad de la información (SGSI), modelo de madurez y el estándar ISO/IEC 27001 de 2013 y 27002 fue suficiente para poder crear un software capaz de medir y calificar el estado de la seguridad de la información de una organización.

- Después de evaluar la norma ISO/IEC 27001:2005 en conjunto con los niveles de madurez fue posible determinar que si se cumple como mínimo la norma a un nivel general ADMINISTRADO una organización puede pensar en optar por una certificación.

- Al momento de diseñar la herramienta se concluyó que una aplicación WEB era la mejor opción, debido a que se podía tener una mejor administración de la Base de Datos en donde se aloja toda la información de los cuestionarios, además que nos permite un mayor control de acceso (seguridad); Por todo esto se decidió programar la herramienta utilizando lenguajes de programación como: PHP, HTML, Java Script, entre otros.

- Al probar la herramienta con diferentes organizaciones, se pudo apreciar con gran agrado que la seguridad de la información es un tema que toma cada vez más protagonismo en las políticas y procedimientos generales donde aún en las organizaciones pequeñas se tiene conocimiento de algunos controles de seguridad.

- Antes de iniciar un proceso de auditoría informática o un análisis de riesgos en una organización es importante identificar todos los factores relacionados con su área informática: hardware, software, infraestructuras, redes y personal, además de los elementos que hacen parte de su medio ambiente.

- La aplicación de este software y sus resultados ayuda a las organizaciones a crear planes de mejora y de contingencia a través del conocimiento de sus aspectos más débiles de seguridad y a tener en cuenta las recomendaciones de la ISO 27002:2013.

10. RECOMENDACIONES

- Tener en cuenta los reportes que genera el programa, y que estos sirvan a modo de guía para implementar unos mejores controles a los riesgos que se vea expuesta una organización.

- A cualquier organización que haga uso del software EVA27 debería repetir el proceso de resolver los cuestionarios pero de una manera más detallada con la participación de los encargados específicos de cada área para obtener resultados más exactos y se cumpla mucho mejor la intención del software.

- Estudiantes y todo tipo de personas interesadas en el tema de seguridad de la información deberían acceder a la herramienta que esta conferida con intención académica y de la misma forma que otras personas comparten información sobre estos temas este software es también un aporte destinado a crecer y actualizarse para seguir siendo útil.

- Se debe estar atentos a cambios en la norma ya sea que se distribuyan los controles de formas distintas o se agreguen nuevos temas de evaluación para así mismo realizar los cambios respectivos en la Base de Datos de la herramienta, y de ser necesario, en la codificación del mismo.

- Hacer uso de todos los tipos de reporte más específicos de la herramienta con el fin de detectar exactamente cuáles son los puntos que se deben mejorar en cuanto al SGSI.

11. REFERENCIAS

27001-online.com. (s.f.). *ISO 27001 Online*. Recuperado el 26 de 05 de 2014, de http://www.27001-online.com/

BENAVIDES RUANO, M. C. (2013). *RIESGOS Y CONTROL INFORMÁTICO.* San Juan de Pasto: Universidad Nacional Abierta y a Distancia UNAD.

BSIGROUP. (16 de 5 de 2014). *Seguridad de la Información ISO 27001.* Obtenido de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-degestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/

BUITRAGO ESTRADA, J. C., BONILLA PINEDA, D. H., & MURILLO VARON, C. E. (2012). *DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001.* Bogota: UNIVERSIDAD EAN.

Calder, A. (2006). *Nueve claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001.* Bogotá, Colombia: Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC.

ICONTEC. (2006). *Norma técnica colombiana ISO/IEC 27001, COMPENDIO, Sistema de Gestión de la seguridad de la información.*

IT GOVERNANCE INSTITUTE. (16 de 6 de 2014). *COBIT® 4.1 Spanish. ITGI, 2007.* Obtenido de http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx

organization, O. (2013). *OWASP Top 10*. Recuperado el 06 de 2015, de The Ten Most Critical Web Application Security Risk: https://www.owasp.org/index.php/Main_Page

Pressman, R. S. (2002). *Ingeniería de software: un enfoque práctico.* Madrid (España): McGrawhill, Quinta Edición.

SegTec. (2009). *SEGURIDAD Y TECNOLOGÍA, Preguntas y respuestas sobre ISO 17799. (2008).* Recuperado el 22 de 05 de 2014, de www.segtec.net: http://www.segtec.net/2009/11/todo-sobre-la-iso-17799/

SUAREZ SIERRA, L. P., & AMAYA TARAZONA, C. A. (2013). *SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI.* Bogotá: Universidad Nacional Abierta y a Distancia.

Universidad de Vigo, España. (s.f.). *Área de ciencias e investigación, Familia de normas ISO/IEC 27000, .* Recuperado el 18 de 5 de 2014, de http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

EVA27 - MANUAL DE USUARIO

marzo 28

2016

Este documento presenta las características principales del software EVA27, su acceso y su uso por parte del usuario auditor de tal forma que pueda administrar el desarrollo de la evaluación de SGSI de la organización.

GUÍA RÁPIDA DEL USUARIO

CONTENIDO

		Pg.
1.	INTRODUCCIÓN	2
2.	BOTONES	3
3.	MANUAL DEL USUARIO	5
3.1.	PÁGINA PRINCIPAL	7
3.2.	PÁGINA DE INICIO	8
3.3.	PROYECTO	9
3.4.	ESTADÍSTICAS	
3.5.	CUESTIONARIOS	10
3.6.	REPORTES	13
3.7.	ASISTENTE DE REPORTES	14

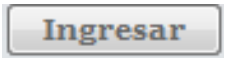
1. INTRODUCCIÓN

El manual de usuario es un documento que tiene como objetivo dar un apoyo y ayuda constante a el usuario final, explicando las características principales que posee cada módulo o proceso del sistema WEB denominado EVA27.

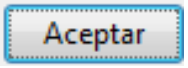
La aplicación ha sido creada para que el responsable del sistema de gestión de la seguridad de la información (SGSI) de la organización u otro relacionado, pueda medir el nivel de madurez de este a través de la contestación de diferentes cuestionarios para que con las respuestas de estos se puedan generar reportes que expliquen gráfica y textualmente los puntos más fuertes y más débiles de la organización tomando como referencia los dominios, objetivos de control y controles de la norma ISO 27001 de 2013 y las recomendaciones sobre su aplicación descritas en la norma ISO 27002 del mismo año.

A partir de los resultados obtenidos la organización tendrá más fácil tomar decisiones y buscar las acciones que ayuden a fortalecer la seguridad de la información y por ende, la calidad de los productos o servicios ofrecidos, además de lo anterior este software pretende ser un punto importante de partida para que una empresa pueda optar por una certificación.

2. BOTONES



Permite entrar a la aplicación



Permite aceptar alguna acción o proceso específico.

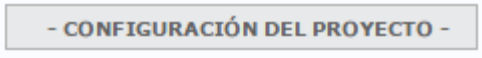
Permite ir a la página de inicio de la aplicación.

Permite ir a la página donde están los cuestionarios.

Despliega los objetivos de control contenidos en este dominio.

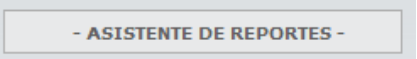
Permite ir a los cuestionarios de control que contenga un objetivo de control.

Acceso a las estadísticas del proyecto

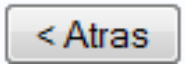


Abre la ventana de configuración de proyecto para seleccionar los dominios que serán evaluados.

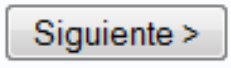
Acceso a la ventana de reportes y al estado de resolución de los cuestionarios



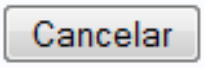
Abre la ventana emergente del asistente de reportes



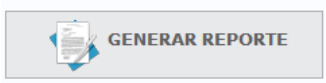
Permite regresar a la anterior vista o anterior ventana de configuración



Permite avanzar a la siguiente ventana de configuración

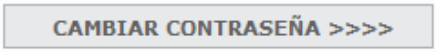


Cierra la ventana emergente

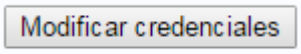


Abre una ventana emergente que permite configurar las opciones del reporte.

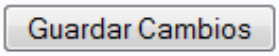
Permite entrar a la configuración de los datos básicos de proyecto y credenciales



Permite ir a los campos de modificación de contraseña



Accede al formulario de modificación de datos básicos de proyecto



Permite guardar los cambios realizados en los datos personales

Permite abrir este documento de ayuda

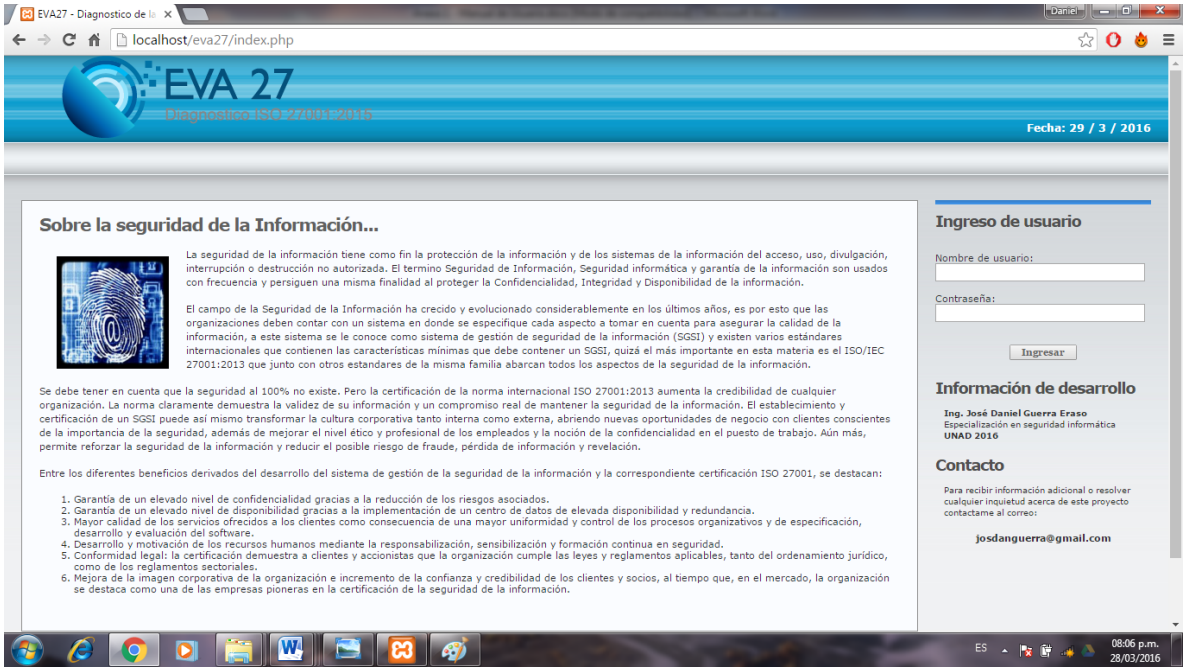
Permite cerrar sesión y nos lleva a la página de entrada

3. MANUAL DEL USUARIO

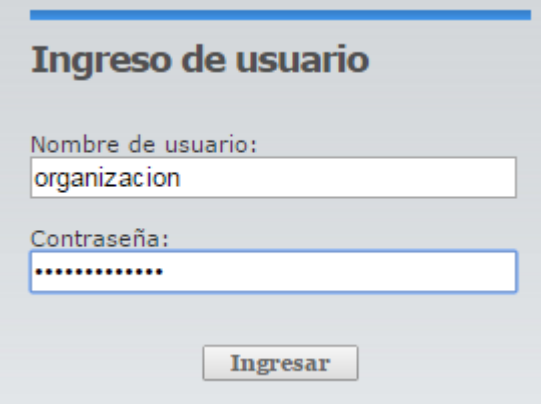
Para ingresar a la herramienta lo primero que se debe hacer es, a través del navegador acceder al vínculo suministrado (puede variar dependiendo de la solicitud y el uso que se le dará), y aparecerá la siguiente página.

3.1 PÁGINA PRINCIPAL

Esta es la página principal de la aplicación y contiene textos que explican, que es la seguridad de la información y los beneficios que traería una certificación en este campo, a través de la norma ISO/IEC 27001:2013.

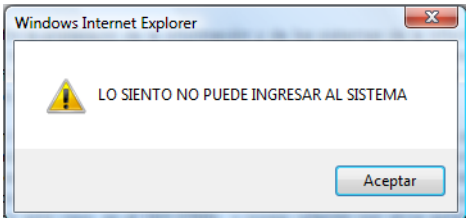


En el panel de la derecha se encuentra el INGRESO DE USUARIO, para poder acceder a las herramientas que nos brinda la aplicación, se debe tener un nombre de usuario y contraseña previamente asignado por los desarrolladores, se ingresan en los campos correspondientes y se oprime el botón ingresar, así:



Si no se cuenta con datos de ingreso, pueden ser solicitados poniéndose en contacto con los desarrolladores al correo josdanguerra@gmail.com, se evaluará el caso y se asignaran los datos de usuario que son necesarios para tener acceso a la aplicación.

Si el nombre de usuario y/o contraseña están mal digitados aparecerá la siguiente ventana.

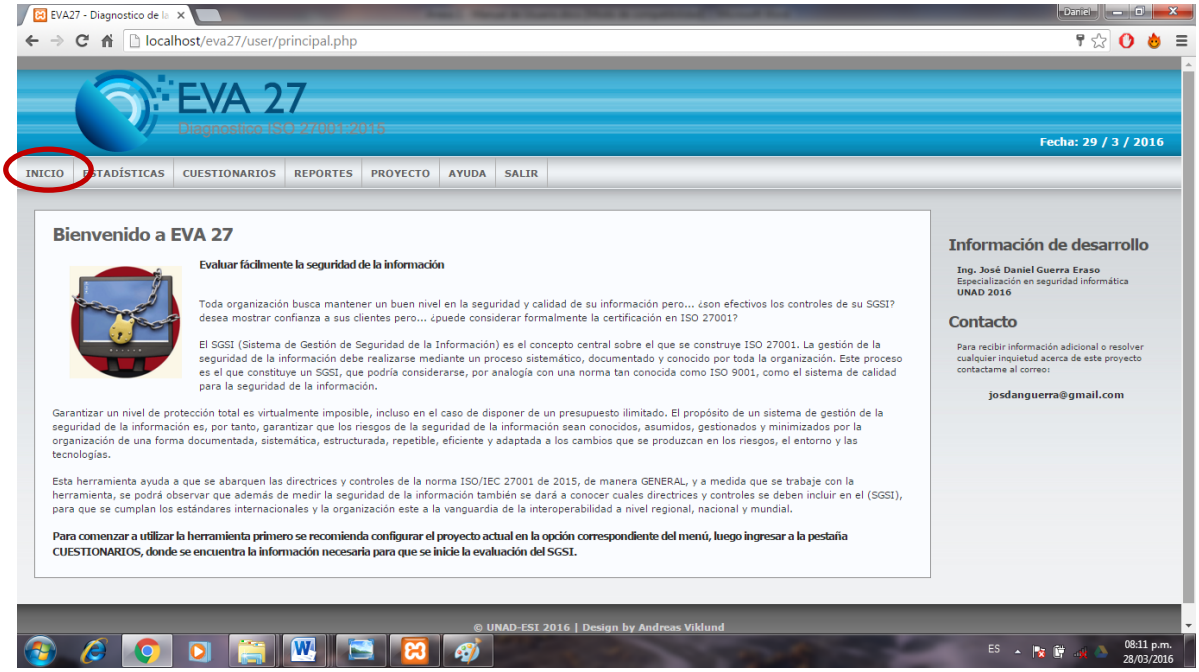


Se da clic en aceptar para realizar un nuevo intento de ingreso.

3.2 PÁGINA DE INICIO

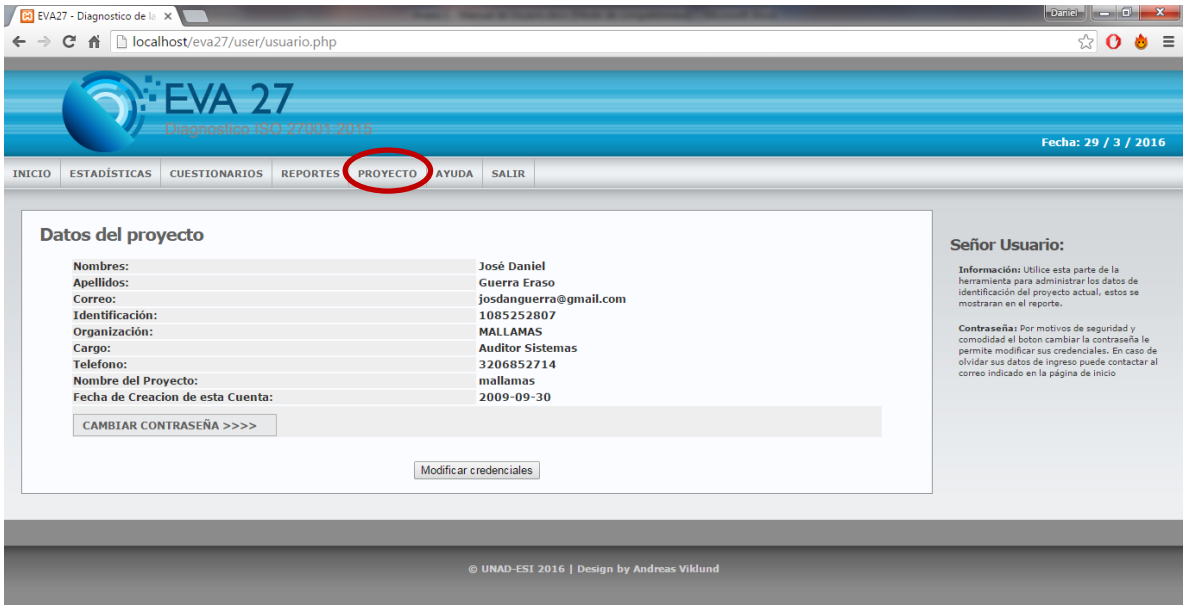
Cuando el nombre de usuario y contraseña son válidas se accede a la página de inicio de la aplicación, donde aparecerá una bienvenida al sistema y se encontrará información de lo que está en capacidad de hacer la herramienta.

Si es la primera vez que se ingresa a la herramienta se recomienda verificar que lo datos del proyecto sean correctos, para este fin se ingresa a la pestaña **PROYECTO**, la cual lleva al módulo donde se encuentran los datos del mismo.

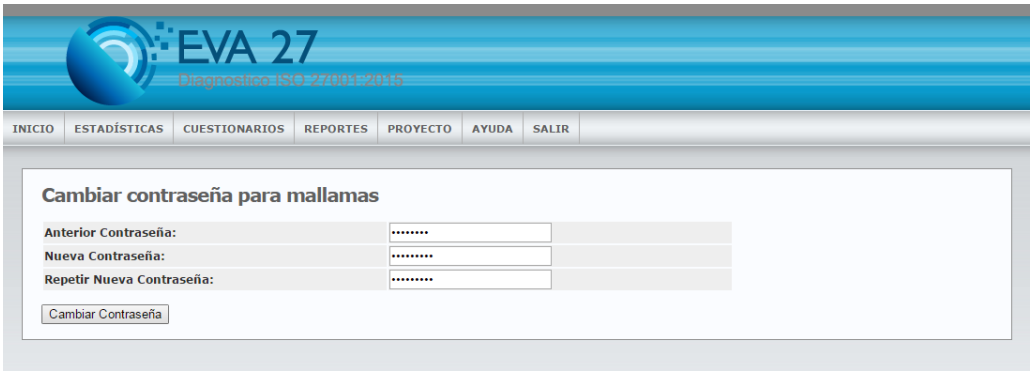


3.3 PROYECTO

Si se quiere modificar algún dato que este mal o este desactualizado se presiona el botón Modificar datos personales, este lleva a la página donde se podrá modificar casi toda la información excepto la que está de un color gris, es decir, no se podrá modificar el número de identificación y la fecha de creación de la cuenta, al terminar de realizar los cambios se da clic en el botón Guardar Cambios.

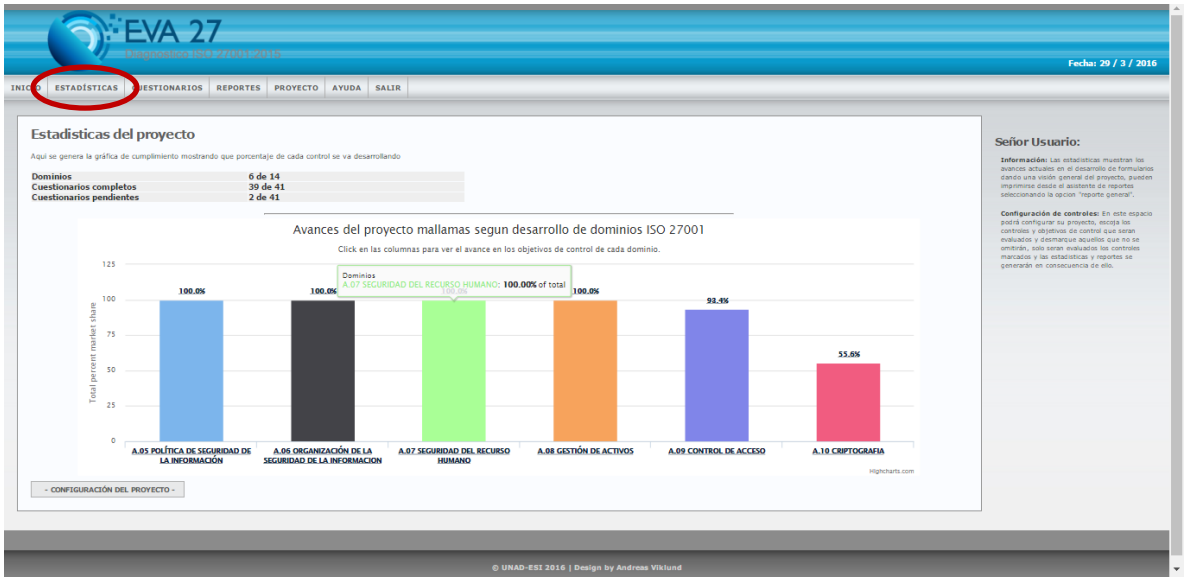


Si se desea, se puede cambiar la contraseña que fue asignada por los desarrolladores, para esto se da clic al botón de cambiar contraseña, de ahí se pasa a la página donde se ingresa los datos para el respectivo cambio, aquí se solicita la contraseña anterior y se pide que digitar en 2 campos separados la nueva contraseña, al terminar se da clic en el botón Cambiar Contraseña con lo que finaliza esta operación.



3.4 ESTADÍSTICAS

En este apartado el usuario podrá explorar las características del estado de resolución de los cuestionarios tanto para cada dominio como para cada objetivo de control, cantidad de cuestionarios resueltos y pendientes, cantidad de hallazgos, etc.



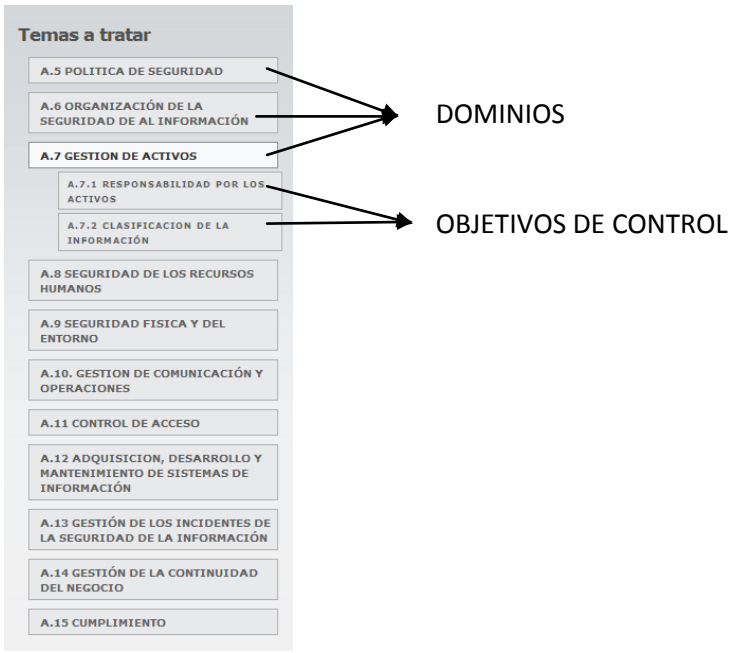
En esta página también puede configurarse el proyecto con el botón “Configuración de proyecto” cuyo fin es que las organizaciones puedan seleccionar los dominios que le sean relevantes y descartar aquellos que no requieren una revisión, esta característica esta pensada en que distintas organizaciones pueden no tener la necesidad de evaluar completamente la norma, en cualquier momento se puede acceder a esta opción y modificar las opciones de configuración

NOTA: La decisión tomada en la configuración afectará toda la aplicación y los datos que se muestren serán sobre los dominios activos

3.5 CUESTIONARIOS

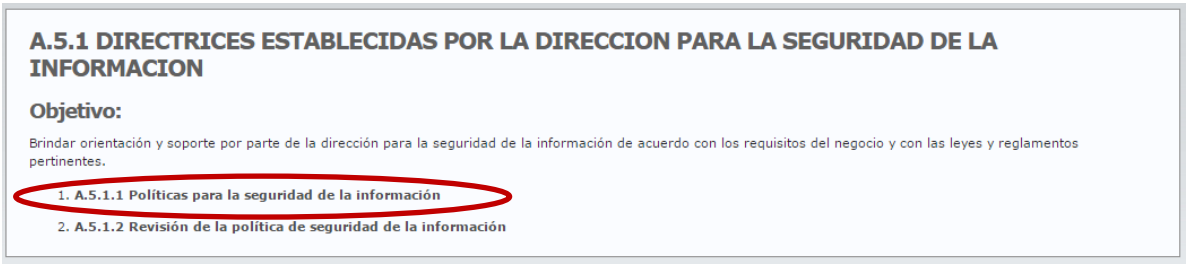
Para comenzar la evaluación del sistema de gestión de seguridad de la información (SGSI), se debe ingresar a la pestaña de cuestionarios, en esta se puede observar información de los dominios y objetivos de control que componen los cuestionarios basados en la norma además se explica cómo se debe calificar las preguntas de los cuestionarios siguiendo el modelo de madurez.

En el panel ubicado a la derecha de la página de cuestionarios se encuentran once (11) botones con los 11 temas que contiene la norma ISO 27001, al dar clic en cualquiera de estos botones se desplegará hacia su parte inferior, botones con los subtemas de dicho tema, cabe anotar que todos los temas no tienen el mismo número de subtemas.



Cuando se despliegan un objetivo de control seleccionado aparecerá en el panel principal la descripción de dicho objetivo de control y la lista de cuestionarios de control que contiene.

Los cuestionarios se encuentran en forma de lista y tienen un vínculo a la ventana emergente donde están los preguntas, el número de cuestionarios y preguntas depende del dominio y objetivo de control, lo que quiere decir que todos no tienen el mismo número de cuestionarios ni de preguntas.



Estando aquí, se procede a seleccionar el cuestionario que se desee calificar, este nos aparecerá en una ventana emergente.

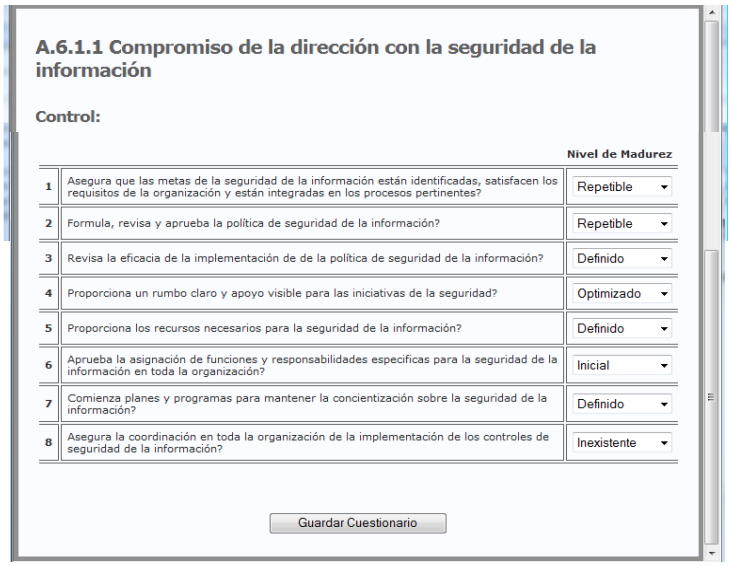
En dicha ventana de cuestionario aparecerá el numeral y nombre del cuestionario, además, el control que debe tener implementado.

Para determinar en qué nivel se encuentra clasificado el cuestionario aparecerá más abajo una serie de preguntas, las cuales tienen a su lado derecho un menú desplegable que corresponde al nivel de madurez, con 6 (seis) posibles respuestas, que van desde inexistente siendo el más bajo,

hasta optimizado que es el nivel más alto (estos niveles de madurez son tomados de las directrices generales de COBIT).

Al terminar de evaluar el cuestionario se debe dar clic en el botón Guarda Cuestionario, el cual está ubicado en la parte inferior de la ventana.

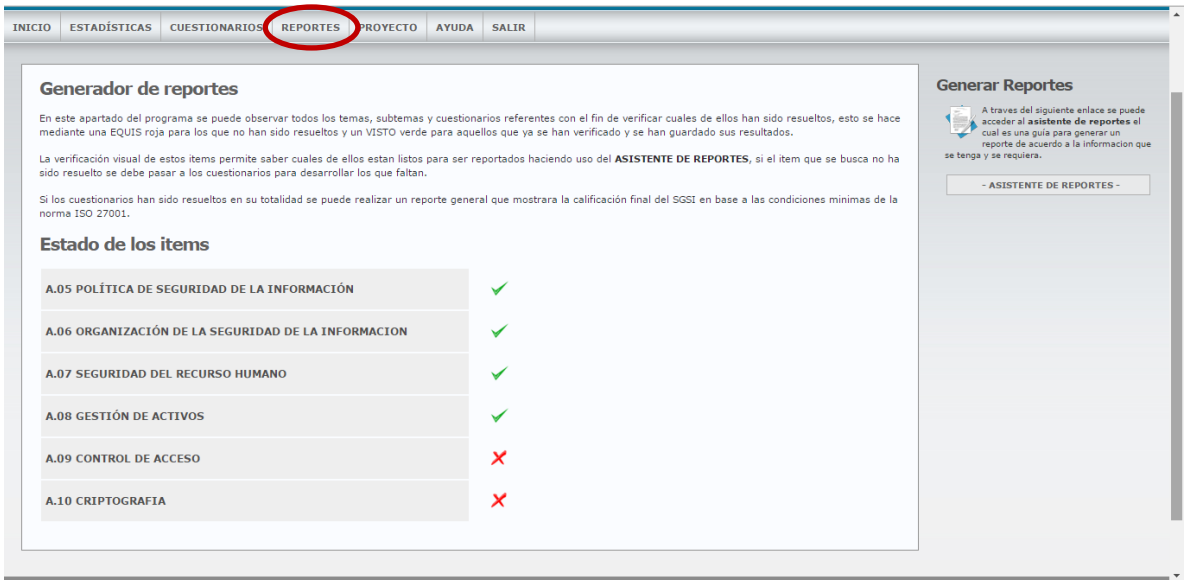
La información de los cuestionarios es modificable en cualquier momento con el fin de que a medida que evoluciona la investigación del estado del SGSI se pueda actualizar los avances y generar reportes completamente nuevos sobre la nueva situación de la institución respecto al estándar internacional ISO 27001; la ventana emérgete de los cuestionarios aparece de la siguiente forma:



3.6 REPORTES

Cuando se tengan contestados completamente los cuestionarios de un objetivo de control, dominio o de todos los dominios activos, se puede proceder al módulo de reportes en donde se puede generar un informe basado en las respuestas que se han colocado en los cuestionarios.

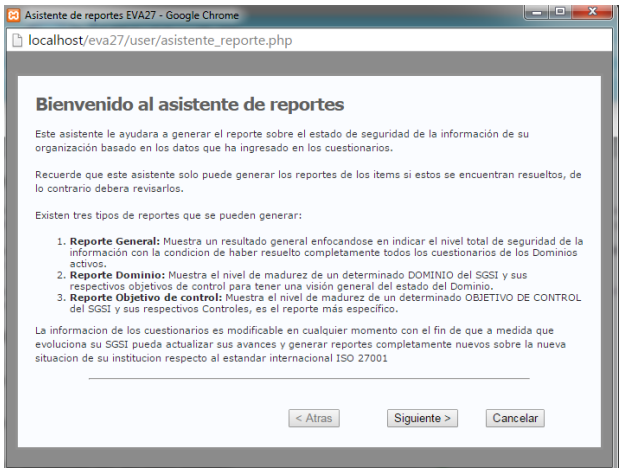
En la página de reportes está el listado de los dominios, objetivos y cuestionarios de los controles, donde se puede observar su estado de la siguiente forma: si ya están contestados tendrá un VISTO verde (✓), de lo contrario tendrá una EQUIS roja (✗), aplicándose este tipo de información tanto para cuestionarios como para temas y subtemas. Esta página se verá así:



3.7 ASISTENTE DE REPORTES

Al tener claro que temas y/o subtemas se encuentran ya evaluados se procede a generar el reporte, para esto se ubica en el panel derecho de la página de reportes el botón del Asistente de Reportes.

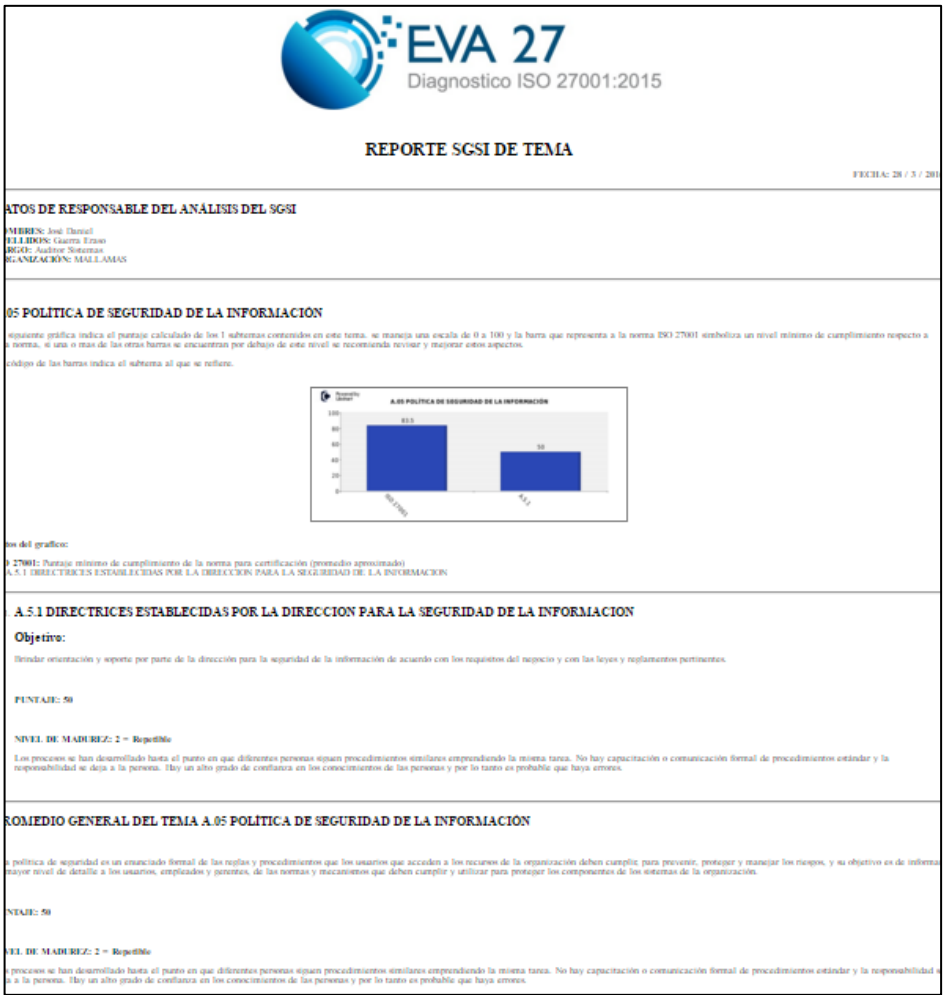
Al oprimir el botón del Asistente de Reportes aparecerá una ventana emergente con información de cuáles son los requisitos para comenzar a generar el reporte y que tipos de reporte se pueden realizar.



Al dar clic en el botón siguiente, aparecerá la siguiente ventana:

En esta ventana, primero se debe seleccionar el tipo de reporte, entre: Reporte General, Reporte por Tema o Reporte por Subtema; si se selecciona una de las 2 últimas opciones, se tendrá al lado derecho un menú desplegable con los dominios u objetivos de control que ya se encuentren totalmente evaluados, se selecciona uno de ellos y se da clic en siguiente:

Esta ventana indica el nombre del tema o subtema y el tipo de reporte que esta por generarse, para esto se da clic en el botón GENERAR REPORTE, al hacer esto saldrá otra ventana con la información resultante del procesamiento de la evaluación de los cuestionarios, la ventana se verá de la siguiente forma:



EVA 27
Diagnostico ISO 27001:2015

REPORTE SGSI DE TEMA

FECHA: 28 / 5 / 201

ATOS DE RESPONSABLE DEL ANÁLISIS DEL SGSI

MBRES: José Daniel
ELLIDOS: Guerra Erazo
RGO: Auditor Sistemas
GANIZACIÓN: MALLAMAS

05 POLITICA DE SEGURIDAD DE LA INFORMACIÓN

siguiente gráfica indica el puntaje calculado de los 1 subtemas contenidos en este tema. se maneja una escala de 0 a 100 y la barra que representa a la norma ISO 27001 simboliza un nivel mínimo de cumplimiento respecto a
a norma, si una o mas de las otras barras se encuentran por debajo de este nivel se recomienda revisar y mejorar estos aspectos.

ódigo de las barras indica el subtema al que se refiere.

os del grafico:

27001: Puntaje mínimo de cumplimiento de la norma para certificación (promedio aproximado)
A.5.1 DIRECTRICES ESTABLECIDAS POR LA DIRECCION PARA LA SEGURIDAD DE LA INFORMACION

A.5.1 DIRECTRICES ESTABLECIDAS POR LA DIRECCION PARA LA SEGURIDAD DE LA INFORMACION

Objetivo:

Brindar orientación y soporte por parte de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

PUNTAJE: 50

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

ROMEDIO GENERAL DEL TEMA A.05 POLITICA DE SEGURIDAD DE LA INFORMACION

a política de seguridad es un enunciado formal de las reglas y procedimientos que los usuarios que acceden a los recursos de la organización deben cumplir, para prevenir, proteger y manejar los riesgos, y su objetivo es de informa
mayor nivel de detalle a los usuarios, empleados y gerentes, de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

NTAJE: 50

EL DE MADUREZ: 2 = Repetible

s procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad s
a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

La información del reporte se divide en secciones, en la primera están los datos del responsable del análisis y evaluación del SGSI, en la segunda está el nombre del dominio u objetivo evaluado y su descripción, en la tercera parte está la gráfica la cual tiene en la primera barra el puntaje mínimo exigido por la norma ISO 27001 para llegar a una certificación, y en las barras siguientes estarán representadas los valores, de los cuestionarios de control, objetivos de control o dominios (según el tipo de reporte), en una escala de 0-100 y clasificada en un nivel de madurez.

En la cuarta sección estarán descritos los dominios u objetivos, esta explicación incluye el control que tenga, el puntaje obtenido, y el nivel de madurez promedio en una escala de 0 – 5 con la respectiva explicación del nivel en que se clasifique el ítem.

Se finaliza en una quinta sección donde está la descripción del objetivo de control, el modelo de madurez, y el puntaje general promedio del dominio u objetivo evaluado.

ISO/IEC 27002 section	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
5	**Security policy**									
5.1	**Information security policy**									
5.1.1	Information Security Policy document	P	P	P		P	P	P	P	P
5.1.2	Review of the information security policy	P	P	P		P	P	P	P	P
6	**Organization of information security**									
6.1	**Internal Organization**									
6.1.1	Management commitment to information security	P	P	P		P	P	P	P	P
6.1.2	Information security coordination		P	P		P	P	P	P	P
6.1.3	Allocation of information security responsibilities		P	P	P	P	P	P	P	P
6.1.4	Authorization process for information processing facilities		P					P	P	P
6.1.5	Confidentiality agreements		P	P				P		
6.1.6	Contact with authorities		P			P		P	P	P
6.1.7	Contact with special interest groups		P	P	P			P	P	P
6.1.8	Independent review of information security		P	P	P	P	P	P	P	P
6.2	**External Parties**									
6.2.1	Identification of risks related to external parties	P	P	P				P	P	P
6.2.2	Addressing security when dealing with customers	P	P	P				P	P	P
6.2.3	Addressing security in third party agreements	P	P	P	P	P	P	P	P	P
7	**Asset Management**									
7.1	**Responsibility for Assets**									
7.1.1	Inventory of Assets		P	P			P	P	P	P
7.1.2	Ownership of assets		P	P	P	P	P	P	P	P
7.1.3	Acceptable use of assets		P	P				P	P	P
7.2	**Information classification**									
7.2.1	Classification guidelines		P						P	P
7.2.2	Information labelling and handling	P		P	P			P	P	P
8	**Human Resources Security**									
8.1	**Prior to employment**									
8.1.1	Roles and responsibilities	P	P	P				P	P	
8.1.2	Screening	P	P					P	P	P
8.1.3	Terms and conditions of employment	P	P					P	P	P
8.2	**During employment**									
8.2.1	Management responsibilities	P	P	P	P			P	P	P
8.2.2	Information security awareness, education and training	P	P	P	P			P	P	P
8.2.3	Disciplinary process	P	P	P	P			P	P	P
8.3	**Termination or change of employment**									
8.3.1	Termination responsibilities		P	P				P	P	P
8.3.2	Return of assets		P					P	P	P
8.3.3	Removal of access rights		P	P				P	P	P
9	**Physical and Environmental Security**									
9.1	**Secure Areas**									
9.1.1	Physical security perimeter	P	P	P				P	P	P
9.1.2	Physical entry controls	P	P	P	P			P	P	P
9.1.3	Securing offices, rooms and facilities	P	P	P	P			P	P	P
9.1.4	Protecting against external and environmental attacks		P	P						P
9.1.5	Working in secure areas	P		P				P	P	P
9.1.6	Public access, delivery and loading areas	P	P	P				P	P	P
9.2	**Equipment security**									
9.2.1	Equipment siting and protection		P	P	P			P	P	P
9.2.2	Supporting utilities		P	P		P	P			P
9.2.3	Cabling Security			P				P		P
9.2.4	Equipment maintenance		P	P	P				P	P

9.2.5	Security of equipment off-premises		P					P	P	P
9.2.6	Secure disposal or re-use of equipment	P	P	P				P		
9.2.7	Removal of property	P	P	P	P			P	P	P
10	**Communications and Operations Management**									
10.1	**Operational procedures and responsibilities**									
10.1.1	Documented operating procedures		P	P		P	P	P	P	P
10.1.2	Change management	P	P	P				P	P	P
10.1.3	Segregation of duties	P	P	P				P	P	P
10.1.4	Separation of development, test and operational facilities	P	P	P				P	P	P
10.2	**Third party service delivery management**									
10.2.1	Service delivery	P	P	P	P	P	P	P	P	P
10.2.2	Monitoring and review of third party services				P			P	P	P
10.2.3	Managing changes to third party services		P	P				P	P	P
10.3	**System planning and acceptance**									
10.3.1	Capacity management		P							P
10.3.2	System acceptance			P	P					P
10.4	**Protection against malicious and mobile code**									
10.4.1	Controls against malicious code	P		P	P	P	P		P	P
10.4.2	Controls against mobile code		P	P					P	P
10.5	**Back-up**									
10.5.1	Information back-up		P	P			P		P	P
10.6	**Network security management**									
10.6.1	Network controls			P				P	P	P
10.6.2	Security of network services		P	P	P			P	P	P
10.7	**Media handling**									
10.7.1	Management of removeable media	P	P	P				P	P	P
10.7.2	Disposal of media		P	P				P	P	P
10.7.3	Information handling procedures		P	P				P	P	P
10.7.4	Security of system documentation			P				P	P	
10.8	**Exchange of information**									
10.8.1	Information exchange policies and procedures		P	P				P	P	P
10.8.2	Exchange agreements		P	P				P	P	
10.8.3	Physical media in transit		P	P						P
10.8.4	Electronic messaging	P		P				P	P	P
10.8.5	Business information systems	P		P			P	P	P	
10.9	**E-commerce services**									
10.9.1	Electronic commerce	P	P	P				P	P	
10.9.2	On-line transactions	P	P	P				P	P	
10.9.3	Publicily available information			P					P	
10.1	**Monitoring**									
10.10.1	Audit logging	P			P	P		P	P	P
10.10.2	Monitoring system use	P			P	P		P	P	
10.10.3	Protection of log information	P	P	P				P	P	P
10.10.4	Administrator and operator logs	P			P			P	P	P
10.10.5	Fault logging				P		P			P
10.10.6	Clock synchronisation		P	P					P	
11	**Access Control**									
11.1	**Business requirements for access control**									
11.1.1	Access control policy	P		P				P	P	
11.2	**User access management**									
11.2.1	User registration	P	P					P	P	
11.2.2	Privilege management		P	P				P	P	
11.2.3	User password management			P				P	P	
11.2.4	Review of user access rights	P		P	P			P	P	

11.3	**User responsibilities**									
11.3.1	Password use		P	P				P	P	
11.3.2	Unattended user equipment	P		P				P	P	
11.3.3	Clear desk and clear screen policy		P	P				P		
11.4	**Network access control**									
11.4.1	Policy on use network services		P	P				P	P	
11.4.2	User authentication for external connections	P	P	P				P	P	
11.4.3	Equipment identification in networks	P	P	P				P	P	
11.4.4	Remote diagnostic and configuration port protection		P	P				P	P	P
11.4.5	Segregation in networks	P		P				P	P	
11.4.6	Network connection control	P		P				P	P	
11.4.7	Network routing control	P		P				P	P	
11.5	**Operating system access control**									
11.5.1	Secure log-on procedures	P	P	P				P	P	
11.5.2	User identification and authentication	P		P				P	P	
11.5.3	Password management system	P		P				P	P	
11.5.4	Use of system utilities			P				P	P	P
11.5.5	Session time-out	P		P		P		P	P	
11.5.6	Limitation of connection time	P	P					P	P	
11.6	**Application and information access control**									
11.6.1	Information access restriction	P		P				P	P	
11.6.2	Sensitive system isolation	P		P				P	P	
11.7	**Mobile computing and teleworking**									
11.7.1	Mobile computing and communications			P				P	P	P
11.7.2	Teleworking			P				P	P	
12	**Information systems acquisition, development and maintenance**									
12.1	**Security requirements of information systems**									
12.1.1	Security requirements analysis and specification		P					P	P	P
12.2	**Correct processing in applications**									
12.2.1	Input data validation		P						P	
12.2.2	Control of internal processing			P					P	
12.2.3	Message integrity		P						P	
12.2.4	Output data validation			P					P	
12.3	**Cryptographic controls**									
12.3.1	Policy on the use of crhptographic controls		P					P	P	
12.3.2	Key management		P					P	P	
12.4	**Security of system files**									
12.4.1	Control of operational software		P					P	P	P
12.4.2	Protection of system test data			P					P	
12.4.3	Access control to program source code		P	P					P	
12.5	**Security in development and support processes**									
12.5.1	Change control procedures		P						P	P
12.5.2	Technical review of applications after operating system changes				P				P	
12.5.3	Restrictions on changes to software packages		P	P					P	
12.5.4	Information leakage		P	P				P		
12.5.5	Outsourced software development	P	P	P				P	P	
12.6	**Technical Vulnerability Management**									
12.6.1	Control of technical vulnerabilities		P						P	
13	**Information security incident management**									
13.1	**Reporting information security events and weaknesses**									
13.1.1	Reporting information security events				P	P		P	P	P
13.1.2	Reporting weaknesses	P			P			P	P	P
13.2	**Management of information security incidents and improvements**									
13.2.1	Responsibilities and procedures					P	P	P	P	P

13.2.2	Learning from information security incidents		P				P	P	P	P
13.2.3	Collection of evidence	P		P		P		P	P	P
14	**Business Continuity management**									
14.1	**Information security aspects of business continuity management**									
14.1.1	Including information security in the business continuity management process		P			P	P			P
14.1.2	Business continuity and risk assessment		P			P	P			P
14.1.3	Developing and implementing continuity plans including information security						P			P
14.1.4	Business continuity planning framework					P	P			P
14.1.5	Test maintaining and re-assessing business continuity plans					P	P			P
15	**Compliance**									
15.1	**Compliance with legal requirements**									
15.1.1	Identification of applicable legislation			P				P	P	P
15.1.2	Intellectual Property Rights (IPR)			P				P		
15.1.3	Protection of organisational records			P		P	P	P	P	P
15.1.4	Data protection and privacy of personal information			P				P		
15.1.5	Prevention of misuse of information processing facilities	P		P						P
15.1.6	Regulation of cryptographic controls			P				P		
15.2	**Compliance with security policies and standards, and technical compliance**									
15.2.1	Compliance with security policies and standards	P			P			P	P	P
15.2.2	Technical compliance checking					P		P	P	
15.3	**Information systems audit considerations**									
15.3.1	Information systems audit controls	P			P					P
15.3.2	Protection of information system audit tools			P	P				P	

ENCUESTA SOBRE FUNCIONALIDAD Y CALIDAD DEL SOFTWARE EVA27

Llene los cuadros "RESPUESTA" de cada pregunta, en las respuestas con "SI" o "NO" marque una X en el cuadro correspondiente y en caso de que deba complementar la respuesta por favor llene el cuadro de "Cual" o "Por qué".

RESPONSABLE: _____

ORGANIZACIÓN: _____

a) ¿El entorno de trabajo por medio de navegador es agradable para el desarrollo de los cuestionarios y la obtención de resultados?

Respuesta:

b) ¿El software funciona ágil y presenta resultados de forma eficiente?

Respuesta

c) ¿La división de las funcionalidades es la correcta para el proceso que se realiza?

Respuesta

d) ¿El manual de usuario ofrecido en el botón de AYUDA es suficiente para resolver las dudas sobre el uso de la aplicación?

SI ☐ NO ☐

Por qué?

e) ¿Según su opinión existe en el aplicativo alguna función o módulo que este de más?

SI ☐ NO ☐

Cuál?

f) ¿Según su opinión existe alguna otra función que pueda echarse en falta?

SI ☐ NO ☐

Cuál?

REPORTE SGSI GENERAL

FECHA: 9 / 4 / 2016

DATOS DE RESPONSABLE DEL ANÁLISIS DEL SGSI

NOMBRES: Ing. Armando
APELLIDOS: Coral
CARGO: Coordinador Informática
ORGANIZACIÓN: Emssanar CETEM

REPORTE GENERAL

La siguiente gráfica indica el puntaje calculado de los 9 DOMINIOS, es decir toda la información sobre la seguridad de la información hasta la fecha. se maneja una escala de 0 a 100 y la barra que representa a la norma ISO 27001 simboliza un nivel mínimo de cumplimiento para alcanzar la certificación, si una o mas de las otras barras se encuentran por debajo de este nivel se recomienda generar reportes de cada DOMINIO y tambien de cada Objetivo de Control con el fin de identificar específicamente cuales son las faltas.

El código de las barras indica el DOMINIO al que se refiere.

Datos del grafico:

ISO 27001: Puntaje mínimo de cumplimiento de la norma para certificación (promedio aproximado)
1: A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
2: A.07 SEGURIDAD DEL RECURSO HUMANO
3: A.08 GESTIÓN DE ACTIVOS
4: A.09 CONTROL DE ACCESO
5: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO
6: A.12 SEGURIDAD DE LAS OPERACIONES
7: A.13 SEGURIDAD DE LAS COMUNICACIONES
8: A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
9: A.18 CUMPLIMIENTO

1. A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La organización de la seguridad está orientada a administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades. Además de fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

PUNTAJE: 61.9

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

2. A.07 SEGURIDAD DEL RECURSO HUMANO

La seguridad de los recursos humanos este orientado a reducir los riesgos de error humano, robo, fraude, o uso inadecuado de las instalaciones, además de definiciones de puestos de trabajo y asignación de recursos. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

La seguridad de los recursos humanos también debe garantizar que los usuarios estén al tanto de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la política de seguridad de la información de la organización en el transcurso de sus tareas normales.

PUNTAJE: 52.93

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

3. A.08 GESTIÓN DE ACTIVOS

La gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad. Además de definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

PUNTAJE: 49.2

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

4. A.09 CONTROL DE ACCESO

Un sistema de control de acceso es el que impide el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. También Implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Además debe registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

PUNTAJE: 59.55

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

5. A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física y del entorno está destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
Además debe controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del

Organismo. Y también debe implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

PUNTAJE: 57.18

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

6. ## A.12 SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 56.66

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

7. ## A.13 SEGURIDAD DE LAS COMUNICACIONES

La seguridad de las comunicaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de transferencia de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 67.37

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

8. ## A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio está orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres. Además de asegurar la coordinación con el personal de la organización y los contactos externos que participaran en las estrategias de planificación de contingencias y asignarles funciones para cada actividad definida.

PUNTAJE: 24.05

NIVEL DE MADUREZ: 1 = Inicial

Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.

9. ## A.18 CUMPLIMIENTO

El cumplimiento está destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad.
Además de revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

PUNTAJE: 49.11

NIVEL DE MADUREZ: 2 = Repetible

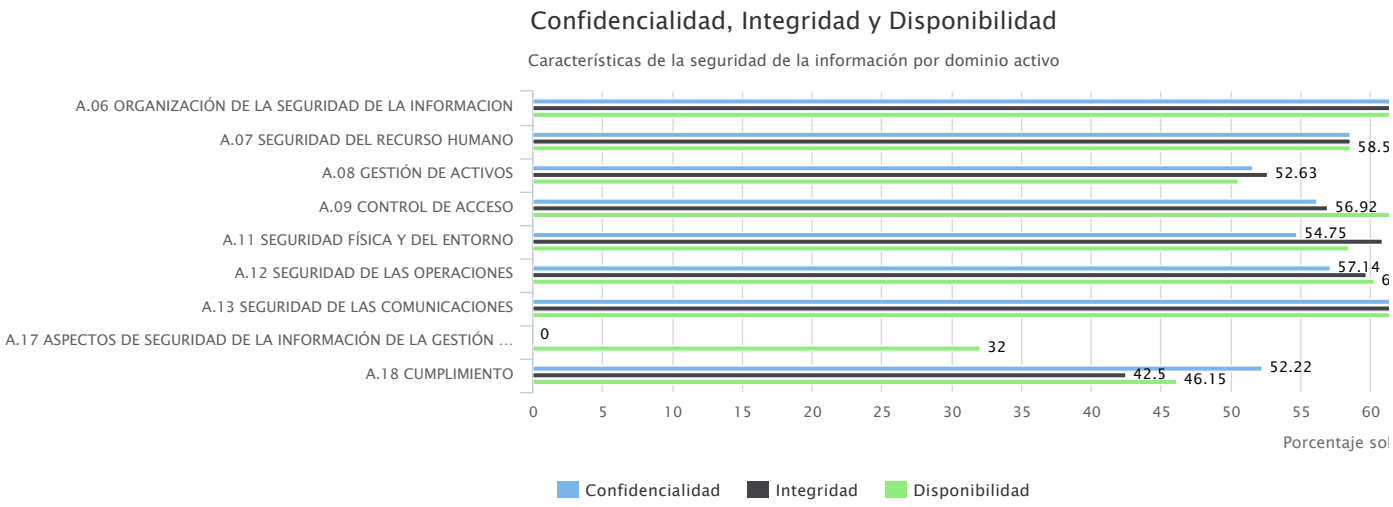
Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

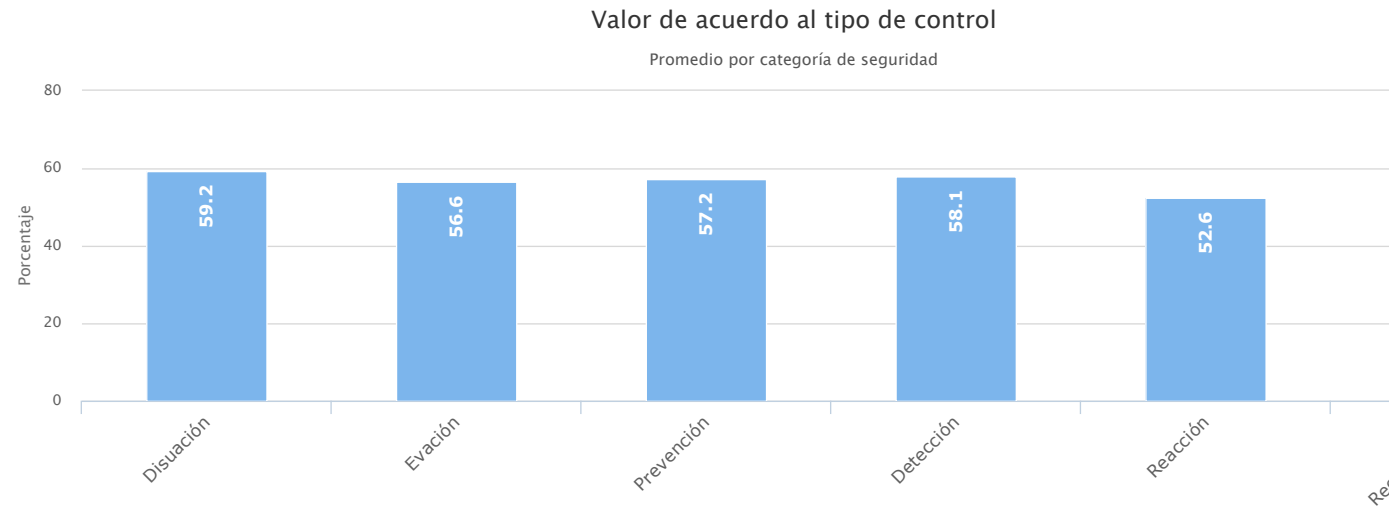
PROMEDIO GENERAL / CALIFICACIÓN FINAL SGSI

PUNTAJE: 53.11

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.





REPORTE SGSI GENERAL

FECHA: 9 / 4 / 2016

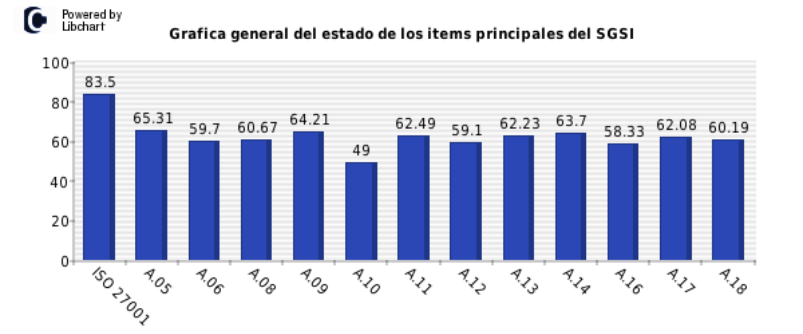
DATOS DE RESPONSABLE DEL ANÁLISIS DEL SGSI

NOMBRES: Luis Carlos
APELLIDOS: Revelo
CARGO: Decano Sistemas
ORGANIZACIÓN: IU CESMAG

REPORTE GENERAL

La siguiente gráfica indica el puntaje calculado de los 12 DOMINIOS, es decir toda la información sobre la seguridad de la información hasta la fecha. se maneja una escala de 0 a 100 y la barra que representa a la norma ISO 27001 simboliza un nivel mínimo de cumplimiento para alcanzar la certificación, si una o mas de las otras barras se encuentran por debajo de este nivel se recomienda generar reportes de cada DOMINIO y tambien de cada Objetivo de Control con el fin de identificar específicamente cuales son las faltas.

El código de las barras indica el DOMINIO al que se refiere.



Datos del grafico:

ISO 27001: Puntaje mínimo de cumplimiento de la norma para certificación (promedio aproximado)
1: A.05 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
2: A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
3: A.08 GESTIÓN DE ACTIVOS
4: A.09 CONTROL DE ACCESO
5: A.10 CRIPTOGRAFIA
6: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO
7: A.12 SEGURIDAD DE LAS OPERACIONES
8: A.13 SEGURIDAD DE LAS COMUNICACIONES
9: A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
10: A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
11: A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
12: A.18 CUMPLIMIENTO

1. A.05 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Una política de seguridad es un enunciado formal de las reglas y procedimientos que los usuarios que acceden a los recursos de la organización deben cumplir, para prevenir, proteger y manejar los riesgos, y su objetivo es de informar al mayor nivel de detalle a los usuarios, empleados y gerentes, de las normas y mecanismos

que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

PUNTAJE: 65.31

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

2. A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La organización de la seguridad está orientada a administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades. Además de fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

PUNTAJE: 59.7

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

3. A.08 GESTIÓN DE ACTIVOS

La gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad. Además de definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

PUNTAJE: 60.67

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

4. A.09 CONTROL DE ACCESO

Un sistema de control de acceso es el que impide el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. También Implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Además debe registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

PUNTAJE: 64.21

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

5. A.10 CRIPTOGRAFIA

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

PUNTAJE: 49

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

6. A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física y del entorno está destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
Además debe controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo. Y también debe implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

PUNTAJE: 62.49

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

7. A.12 SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 59.1

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

8. A.13 SEGURIDAD DE LAS COMUNICACIONES

La seguridad de las comunicaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de transferencia de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 62.23

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

9. A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El desarrollo y mantenimiento de sistemas de información está orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento. Además de definir y documentar las normas y procedimientos que se aplicaran durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan y también determina los métodos de protección de la información crítica o sensible.

PUNTAJE: 63.7

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

10. A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de los incidentes de la seguridad de la información está orientada a minimizar el daño producido por incidentes y anomalías en materia de seguridad, donde también se determina como monitorear dichos incidentes y aprender de los mismos, para no repetir fallos o interrupciones del mismo tipo.

PUNTAJE: 58.33

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

11. A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio está orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres. Además de asegurar la coordinación con el personal de la organización y los contactos externos que participaran en las estrategias de planificación de contingencias y asignarles funciones para cada actividad definida.

PUNTAJE: 62.08

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

12. A.18 CUMPLIMIENTO

El cumplimiento está destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad.
Además de revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

PUNTAJE: 60.19

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

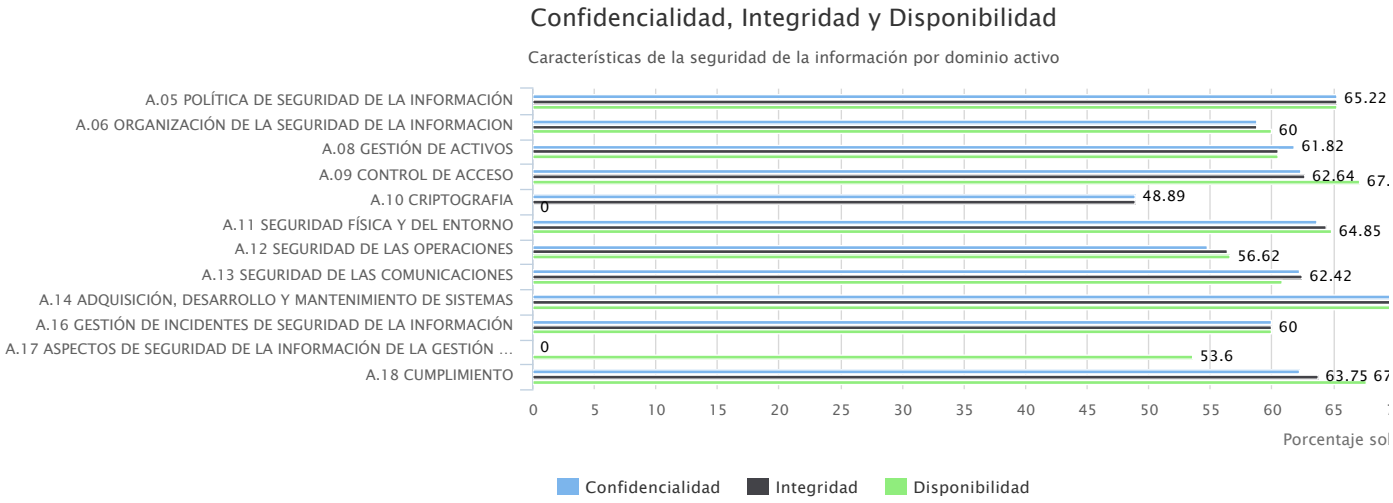
PROMEDIO GENERAL / CALIFICACIÓN FINAL SGSI

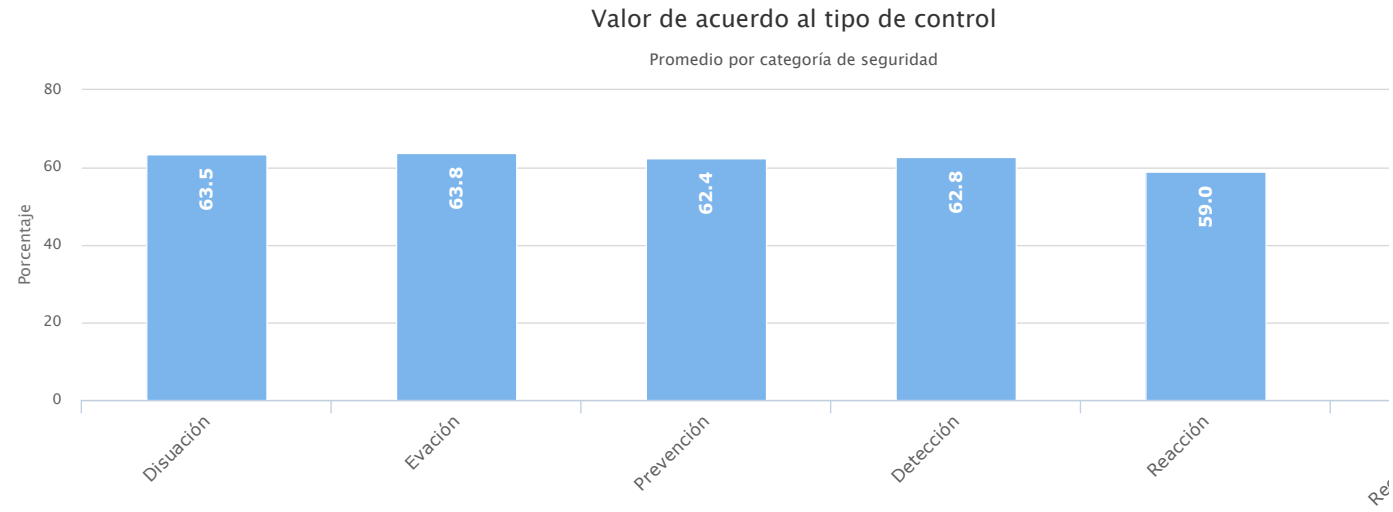
PUNTAJE: 60.58

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento

de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.





REPORTE SGSI GENERAL

FECHA: 9 / 4 / 2016

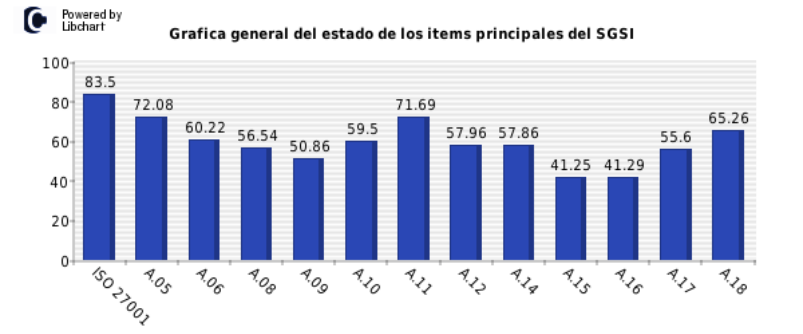
DATOS DE RESPONSABLE DEL ANÁLISIS DEL SGSI

NOMBRES: Jorge Daniel
APELLIDOS: Calderon
CARGO: Auditor Sistemas
ORGANIZACIÓN: MALLAMAS

REPORTE GENERAL

La siguiente gráfica indica el puntaje calculado de los 12 DOMINIOS, es decir toda la información sobre la seguridad de la información hasta la fecha. se maneja una escala de 0 a 100 y la barra que representa a la norma ISO 27001 simboliza un nivel mínimo de cumplimiento para alcanzar la certificación, si una o mas de las otras barras se encuentran por debajo de este nivel se recomienda generar reportes de cada DOMINIO y tambien de cada Objetivo de Control con el fin de identificar específicamente cuales son las faltas.

El código de las barras indica el DOMINIO al que se refiere.



Datos del grafico:

ISO 27001: Puntaje mínimo de cumplimiento de la norma para certificación (promedio aproximado)
1: A.05 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
2: A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
3: A.08 GESTIÓN DE ACTIVOS
4: A.09 CONTROL DE ACCESO
5: A.10 CRIPTOGRAFIA
6: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO
7: A.12 SEGURIDAD DE LAS OPERACIONES
8: A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
9: A.15 RELACIONES CON LOS PROVEEDORES
10: A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
11: A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
12: A.18 CUMPLIMIENTO

1. A.05 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Una política de seguridad es un enunciado formal de las reglas y procedimientos que los usuarios que acceden a los recursos de la organización deben cumplir, para prevenir, proteger y manejar los riesgos, y su objetivo es de informar al mayor nivel de detalle a los usuarios, empleados y gerentes, de las normas y mecanismos

que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

PUNTAJE: 72.08

NIVEL DE MADUREZ: 4 = Administrado

Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.

2. A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La organización de la seguridad está orientada a administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades. Además de fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

PUNTAJE: 60.22

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

3. A.08 GESTIÓN DE ACTIVOS

La gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad. Además de definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

PUNTAJE: 56.54

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

4. A.09 CONTROL DE ACCESO

Un sistema de control de acceso es el que impide el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. También Implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Además debe registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

PUNTAJE: 50.86

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

5. A.10 CRIPTOGRAFIA

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

PUNTAJE: 59.5

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

6. A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física y del entorno está destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
Además debe controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo. Y también debe implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

PUNTAJE: 71.69

NIVEL DE MADUREZ: 4 = Administrado

Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.

7. A.12 SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 57.96

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

8. A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El desarrollo y mantenimiento de sistemas de información está orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento. Además de definir y documentar las normas y procedimientos que se aplicaran durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan y también determina los métodos de protección de la información crítica o sensible.

PUNTAJE: 57.86

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

9. A.15 RELACIONES CON LOS PROVEEDORES

La gestión de comunicación y operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

PUNTAJE: 41.25

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

10. A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de los incidentes de la seguridad de la información está orientada a minimizar el daño producido por incidentes y anomalías en materia de seguridad, donde también se determina como monitorear dichos incidentes y aprender de los mismos, para no repetir fallos o interrupciones del mismo tipo.

PUNTAJE: 41.29

NIVEL DE MADUREZ: 2 = Repetible

Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

11. A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio está orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres. Además de asegurar la coordinación con el personal de la organización y los contactos externos que participaran en las estrategias de planificación de contingencias y asignarles funciones para cada actividad definida.

PUNTAJE: 55.6

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

12. A.18 CUMPLIMIENTO

El cumplimiento está destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad.
Además de revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

PUNTAJE: 65.26

NIVEL DE MADUREZ: 3 = Definido

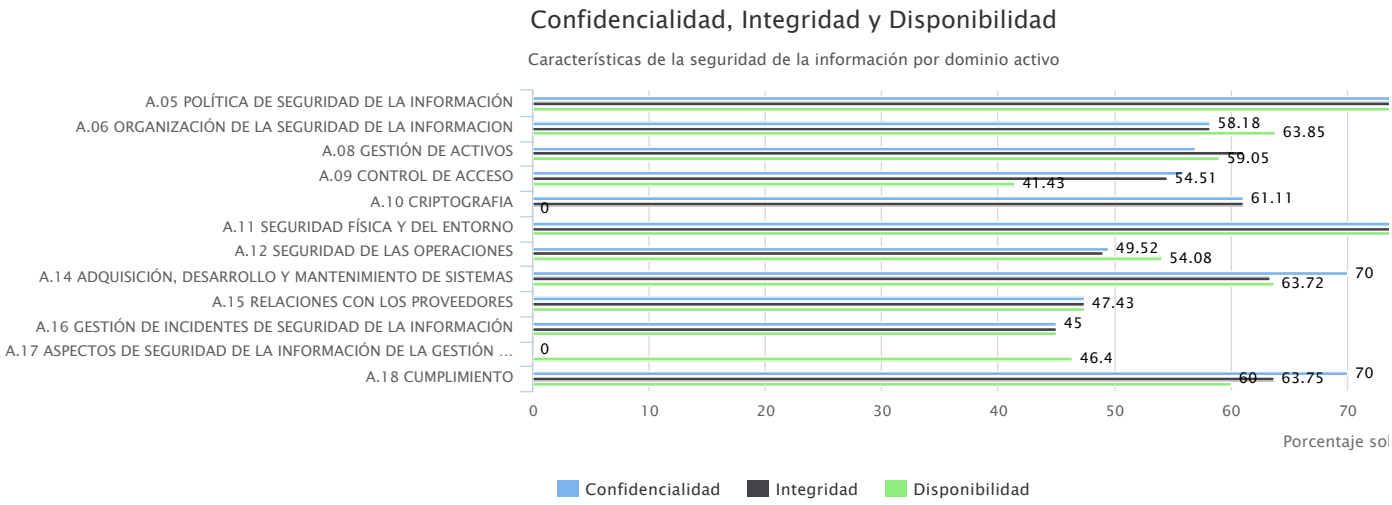
Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

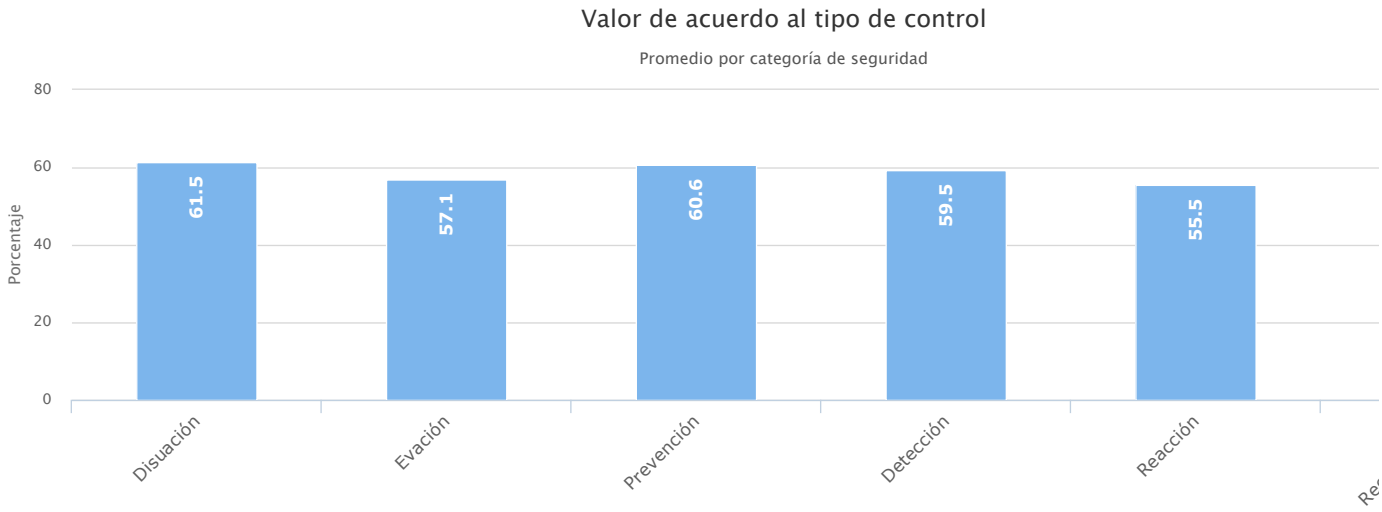
PROMEDIO GENERAL / CALIFICACIÓN FINAL SGSI

PUNTAJE: 57.51

NIVEL DE MADUREZ: 3 = Definido

Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.


Confidencialidad, Integridad y Disponibilidad
Características de la seguridad de la información por dominio activo
A.05 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
A.06 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
A.08 GESTIÓN DE ACTIVOS
A.09 CONTROL DE ACCESO
A.10 CRIPTOGRAFIA
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO
A.12 SEGURIDAD DE LAS OPERACIONES
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
A.15 RELACIONES CON LOS PROVEEDORES
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN ...
A.18 CUMPLIMIENTO
58.18
63.85
59.05
54.51
41.43
61.11
0
49.52
54.08
70
63.72
47.43
45
0
46.4
60
63.75
70
0 10 20 30 40 50 60 70
Porcentaje sol
Confidencialidad
Integridad
Disponibilidad


Valor de acuerdo al tipo de control
Promedio por categoría de seguridad
Porcentaje
80
60
40
20
0
61.5
57.1
60.6
59.5
55.5
Disuación
Evación
Prevención
Detección
Reacción

ENLACE DE ACCESO AL SOFTWARE PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL BASADO EN LA NORMA ISO/IEC 27001 DE 2013

Desarrollado por
Ing. José Daniel Guerra Eraso

DIRECCIÓN: http://pruebaeva27.eshost.com.ar/index.php
USUARIO: "prueba"
CONTRASEÑA: "prueba"

NOTA: El usuario de prueba que se suministra está vacío para efectos de ver el funcionamiento del sistema desde cero, para ver todas las características del software se recomienda activar un solo dominio desde el módulo ESTADÍSTICAS y llenarlo para poder generar reportes rápidamente.

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Programa de Especialización en Seguridad Informática
Pasto, noviembre de 2015