PROTOTIPO GEICO
"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"
BASADO EN LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 17799

LILIANA PATRICIA DUARTE CAMACHO
JOHANNA PEREZ BARBOSA

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2007

PROTOTIPO GEICO
"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"
BASADO EN LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 17799

LILIANA PATRICIA DUARTE CAMACHO
JOHANNA PEREZ BARBOSA

Proyecto para optar al titulo de
Ingeniero de Sistemas

Director:
Mcc. Fernando Antonio Rojas Morales

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2007

Nota de aceptación

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Director

Bucaramanga, 07 de Junio de 2007

DEDICATORIAS

A Dios por haber permitido tener una familia incomparable, a mis padres por haber permitido conocer lo que conozco hasta hoy, por su comprensión en momentos difíciles, por su cariño, por el apoyo y confianza que me han brindado.

LILIANA PATRICIA

A Dios, a mis padres y a mi hermano, por el apoyo, la paciencia, la confianza y el amor que siempre me han brindado, para lograr lo que soy como persona y profesional.

JOHANNA PEREZ

AGRADECIMIENTOS

Es un orgullo para nosotras contar con personas tan maravillosas como lo son nuestros Padres, Amigos, Profesores y Compañeros, que desde un principio nos dieron la colaboración y su apoyo en nuestra orientación profesional y en el desarrollo como persona y por creer en nosotras y hacernos partícipes de su confianza.

Queremos agradecer a los profesores que nos dieron orientación en el transcurso de la carrera y al final de esta, porque con sus críticas constructivas nos ayudaron a salir adelante y a mejorar como profesionales. A nuestras familias por habernos apoyado y servirnos de soporte hasta en los momentos más difíciles, no solo durante ésta etapa sino en todas las etapas vividas. A nuestros amigos por su compañía, colaboración y comprensión.

CONTENIDO

pág.

INTRODUCCIÓN 20

1. SEGURIDAD DE LA INFORMACIÓN 21

1.2 IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN 22

1.3 ¿POR QUÉ ES NECESARIA LA SEGURIDAD DE INFORMACIÓN? 23

1.4 REQUISITOS DE SEGURIDAD DE INFORMACIÓN 24

1.5 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD 25

1.6 SELECCIÓN DE CONTROLES DE SEGURIDAD 26

1.7 PUNTO DE PARTIDA DE LA SEGURIDAD DE LA INFORMACIÓN 27

1.8 FACTORES CRÍTICOS PARA EL ÉXITO DE LA SEGURIDAD DE INFORMACIÓN 28

2. PROBLEMAS DE SEGURIDAD DE INFORMACIÓN 29

2.1 AMENAZAS ACTIVAS 29

2.1.1 Gusanos 29

2.1.2 Bomba Lógica 30

2.1.3 Puertas Trampa 30

2.1.4 Caballo de Troya 30

2.1.5 Bacteria 30

2.1.6 Virus 31

2.2 AMENAZAS PASIVAS 31

2.2.1 Sniffing en Ambiente de Switches 31

2.2.2 Sniffing en ambiente de Switches – Macoff 32

2.2.3 Tempest 32

2.2.4 Ingeniería Social 32

2.2.5 Shoulder Surfing 33

2.2.6 Estaciones abiertas 33

2.2.7 Passwords escritas 33

2.2.8 Dumpster diving 33

3. SERVICIOS DE SEGURIDAD 34

3.1 CARACTERÍSTICAS DE LOS SERVICIO DE SEGURIDAD 34

4. POLÍTICAS DE SEGURIDAD 36

4.1 CARACTERÍSTICAS DE POLÍTICAS DE SEGURIDAD 36

4.1.1 Accesible 36

4.1.2 Definir objetivos de seguridad 36

4.1.3 Definir cada artículo 37

4.1.4 Posición de la organización 37

5. NORMA TÉCNICA SOBRE SISTEMAS DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) 38

6. NORMA TÉCNICA COLOMBIANA NTC-BS 7799-2 39

6.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) 39

6.2 DESARROLLO DE DIRECTRICES PROPIAS DE LOS SGSI 40

7. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 17799 41

7.1 NORMA ISO 17799 41

7.2 ¿A QUIÉN VA DIRIGIDA ISO 17799? 42

7.3 ESTRUCTURA DE LA NORMA ISO 17799 44

7.3.1 Política de seguridad. 45

7.3.2 Aspectos organizativos para la seguridad. 46

7.3.3 Clasificación y control de activos. 46

7.3.4 Seguridad ligada al personal. 46

7.3.5 Seguridad física y del entorno. 46

7.3.6 Gestión de comunicaciones y operaciones. 47

7.3.7 Control de accesos. 47

7.3.8 Desarrollo y mantenimiento de sistemas. 48

7.3.9 Gestión de continuidad del negocio. 48

7.3.10 Conformidad con la legislación. 48

7.4 VENTAJAS DE LA NORMA ISO 17799 48

7.5 BENEFICIOS DE LA NORMA ISO 17799 49

7.6 DOCUMENTACIÓN DE UN SGSI 50

7.6.1 Obstáculos de Documentación SGSI 51

7.6.2 Factores de éxito 52

7.7 IMPLEMENTACIÓN DE UN SGSI 53

8. PROTOTIPO GEICO “SISTEMA DE GESTIÓN DE SEGURIDAD BASADO EN ISO 17799” 54

8.1 ARQUITECTURA Y DISEÑO DEL PROTOTIPO 54

8.1.1 Arquitectura MVC (Modelo/Vista/Control) 56

8.2 ANÁLISIS 58

8.2.1 Modelo Funcional 58

8.2.1.1 Casos de Uso 58

8.3 DISEÑO DEL PROTOTIPO 61

8.3.1 Diseño de Base de Datos 61

8.3.2 Documentación de los casos de uso 61

8.3.3Diseño de Eventos 62

8.3.3.1 Diagrama de Secuencia 62

8.3.3.2 Diagrama de Colaboración 63
8.4 CONSTRUCCIÓN 63

8.4.1 Herramientas de Desarrollo 64

8.5 DESCRIPCIÓN DE PANTALLAS 64

8.5.1 Pantalla Principal 64

8.5.2 Registro de Usuario 66

8.5.3 Información General 66

8.5.4 Glosario 67

8.5.5 Ingresar al sistema (INICIO) 68

8.5.6 Inicio 69

8.5.7 Recopilación de Información 69

8.5.8 Preparación de Auditorias 71

9. CONCLUSIONES 76

BIBLIOGRAFÍA 77

ANEXOS 83

LISTA DE FIGURAS

pág.

Figura 1. Seguridad de Información 24

Figura 2. Proceso de evaluación de riesgo 26

Figura 3. Clasificación de las Empresas Según Norma ISO 17799 43

Figura 4. Riesgo de Sistema de Información 43

Figura 6. Niveles de Documentación SGSI 51

Figura 7. Etapas implementación SGSI 53

Figura 8. Arquitectura de Tres Capas 55

Figura 9. Patrón de Diseño MVC 57

Figura 10. Casos De Uso 58

Figura 11. Inicio del prototipo 65

Figura 12. Evento Registro en Sistema 66

Figura 13. Evento Ver Información del Sistema 67

Figura 14. Evento Ver Glosario 68

Figura 15. Inicio de Sesión 69

Figura 16. Eventos Recopilación Información y Preparación de Auditorias 70

Figura 17. Evento Recopilación de Información 71

Figura 18. Eventos Recopilación Información y Preparación de Auditorias 72

Figura 19. Auditoria 73

Figura 20. Resultados de Auditoria 74

Figura 21. Registro de Evaluación por Usuario 75

Figura 22. Diagrama De Caso De Uso Usuario - Administrador 83

Figura 23. Diagrama de Caso de Uso Administrador Web 84

Figura 24. Diagrama De Secuencia “Verificar Identidad” 95

Figura 25. Diagrama de Colaboración “Verificar Identidad” 96

Figura 26. Diagrama de Secuencia “Ver Información ISO 17799” 96

Figura 27. Diagrama de Colaboración “Ver Información ISO 17799” 97

Figura 28. Diagrama de Secuencia “Ver Glosario” 97

Figura 29. Diagrama de Colaboración "Ver Glosario" 98

Figura 30. Diagrama de Secuencia "Solicitar Pagina" 98

Figura 31. Diagrama de Colaboración "Solicitar Pagina" 99

Figura 32. Diagrama de Secuencia "Registrarse en el sistema" 99

Figura 33. Diagrama de Colaboración "Registrarse en el sistema" 100

Figura 34. Diagrama de Secuencia "Recopilar Información" 100

Figura 35. Diagrama de Colaboración "Recopilar Información" 101

Figura 36. Diagrama de Secuencia "Preparación de Auditorias" 101

Figura 37. Diagrama De Colaboración "Preparación De Auditorias" 102

LISTA DE ANEXOS

pág.

Anexo A. Diagrama de caso de uso 83

Anexo B. Documentación casos de uso 85

Anexo C. Diagrama de secuencia y colaboración 95

GLOSARIO

BS7799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información -no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001.

BSI: Instituto Británico de Normas Técnicas (British Standard Institute)

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002. No es certificable.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SGSI: (Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

RESUMEN

Es de gran importancia que las organizaciones tomen las acciones apropiadas para asegurar la información y los sistemas informáticos con el fin de que estén debidamente protegidos de amenazas y riesgos, por esto es de gran importancia adecuar un Sistemas de Gestión de Seguridad de Información (SGSI) en las empresas de tal forma que se puedan adoptar normas de seguridad, para proteger la información, además con la adecuación del SGSI no solo se gestionaría y se mantendría los activos de información sino que se crearía una cultura de seguridad, de allí nace la necesidad de desarrollar un prototipo en ambiente WEB, que se encargue de medir la seguridad de la información con la que cuenta la empresa, teniendo en cuenta que los diferentes sistemas de información basados en la norma ISO 17799 creados hasta la actualidad han sido hechos para ser accesibles por Internet, utilizando aplicaciones Web, las cuales se han convertido en interfaces de sistemas complejos lo mas parecidas a las aplicaciones de escritorio dando confianza a los usuarios al momento de interactuar con el sistema. El prototipo GEICO (Gestión, Implementación y Control) que se construyó, utiliza aplicaciones Web con el propósito de cumplir con ciertas necesidades, entre las cuales esta que la información sea compartida entre las partes interesadas, de manera que todas tengan acceso a la información completa o aquella parte que les corresponda según su función en cada momento, a su ves se busca que la información sea accesible desde cualquier lugar dentro de la organización e incluso desde el exterior para el encargado de solicitar el servicio del prototipo de Gestión de Seguridad desarrollado, con el fin de evaluar la seguridad con la que cuenta la empresa para que el prototipo le de recomendaciones para mejorar las fallas que tienen referente a la seguridad.

Palabras claves: SGSI, NTC-BS 7799-2, ISO 17799, BS7799.

INTRODUCCIÓN

Actualmente las empresas tienen la necesidad de prepararse para todo tipo de desastre que interrumpa las actividades a las cuales se dedican, en caso de cualquier tipo de desastre las organizaciones estarían propensos a perder clientes y debido a esto las empresas estarían en crisis, un ejemplo de esto seria el caso ocurrido en Estados Unidos debido a el ataque del 11 de septiembre donde se interrumpió todo tipo de actividad de negocio en el país, estos posibles obstáculos causados por caídas de sistemas informáticos, dieron fallas en la información que manejan las empresas dando como resultado la pérdida y el descontrol para manejar las organizaciones debido a la falta de información y control para la toma de decisiones para la continuación de la organización desencadenando la ineficiencia de compromisos establecidos con los clientes, paralizando así todo tipo de negocio de tal forma que se estaría perdiendo credibilidad y eficiencia. De acuerdo a lo anterior es de vital importancia que las empresas cuenten con estrategias de seguridad para la información mitigando todo tipo de riesgo que se pueda presentar.

Además de los desastres ocurridos por vía terrorista o de desastre natural, se puede observar que hay otras amenazas como son: fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad o interrupción de servicio. Uno de estos ataques presentados es la piratería informática que es peor que un desastre ya que no solo daña información, sino que se adecua como una forma de terrorismo, es de allí que nace la necesidad de conocer no solo los procedimientos de protección en una red de datos y su funcionamiento sino también, la ejecución de políticas de seguridad y el establecimiento de mecanismos de vigilancia.

Todo lo anterior debe dar como consecuencia la implantación de una estrategia que asegure la integridad, confidencialidad y disponibilidad de la información, para así evitar el riesgo de alteración de datos o archivos, implantando un Sistema de Gestión de Seguridad de Información (SGSI), encargado de evaluar o determinar riesgos del negocio que resulte de fallas de seguridad, teniendo en cuenta las consecuencias de pérdidas de confidencialidad existentes en la organización, de tal modo que se pueda suplir las perdidas adecuando normas y objetivos de seguridad, evitando que se elimine la información o que simplemente se dañe.

Lo que se busca la norma ISO 17799 al proyecto, es desarrollar un prototipo de información donde se suministre recomendaciones para la gestión de la seguridad de la información por parte de quienes son responsables de generar, implementar y controlar la seguridad de la información en la organización, además con esta aplicación se busca proporcionar una plataforma común para desarrollar normas de seguridad en las empresas, de tal modo que una vez que se conoce el estado actual de la seguridad de la información, se pueda planificar correctamente aspectos que ayuden a mejorar los aspectos que sean determinantes en el mantenimiento de la misma, lo que ayuda al aumento de la seguridad efectiva de los sistemas de información.

1. SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la información es uno e los temas más importantes en los avances tecnológicos a nivel mundial, ya que la información al ser uno de los activos de mayor importancia de las empresas tiende a ser amenazado, provocando que esté a disposición de daños y pérdidas. Se puede ver que a lo largo de la historia el hombre ha tenido la necesidad de transmitir y tratar información de forma continua, y debido a esto se han creado una serie de sistemas que permiten el paso de información sin que se presente pérdida alguna, aunque en muchas ocasiones los sistemas con los que cuenta las empresa tienden a fracasar debido a que en la red pública con la que la mayoría de empresas cuenta esta a disposición de piratas informáticos que tienden a amenazar los datos o archivos de las organizaciones. Asimismo se ha dado la necesidad de implementar servicios, políticas y controles de seguridad en las empresas, permitiendo evaluar los riesgos a los que se ve enfrentada la información y en sí la totalidad de la empresa. De allí nace la necesidad de que las empresas establezcan todo tipo de seguridad basándose en políticas propias para impedir la pérdida de la información.

1.2 IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN

La información es un de los activos más importantes y que tiene valor para la empresa y requiere un resguardo adecuada. La seguridad de la información protege a esta de una amplia gama de peligros, para asegurar la prolongación del negocio, minimizar los daños a la organización y maximizar las inversiones y oportunidades. Por esta razón es de gran importancia que la información preserve

las características de:

a. Confidencialidad: de tal forma que se asegure que la información es accesible solo a quienes están autorizados para ello.
b. Integridad: protección de la exactitud y estado completo de la información y métodos de procesamiento.
c. Disponibilidad: seguridad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Es necesario establecer estos controles para asegurar que se cumplen los objetivos específicos de seguridad de la organización, ya que si la información que se maneja en una empresa no cuenta con alguna de estas características, estaría más propensa a daños, disminuyendo así la continuidad del negocio[1].

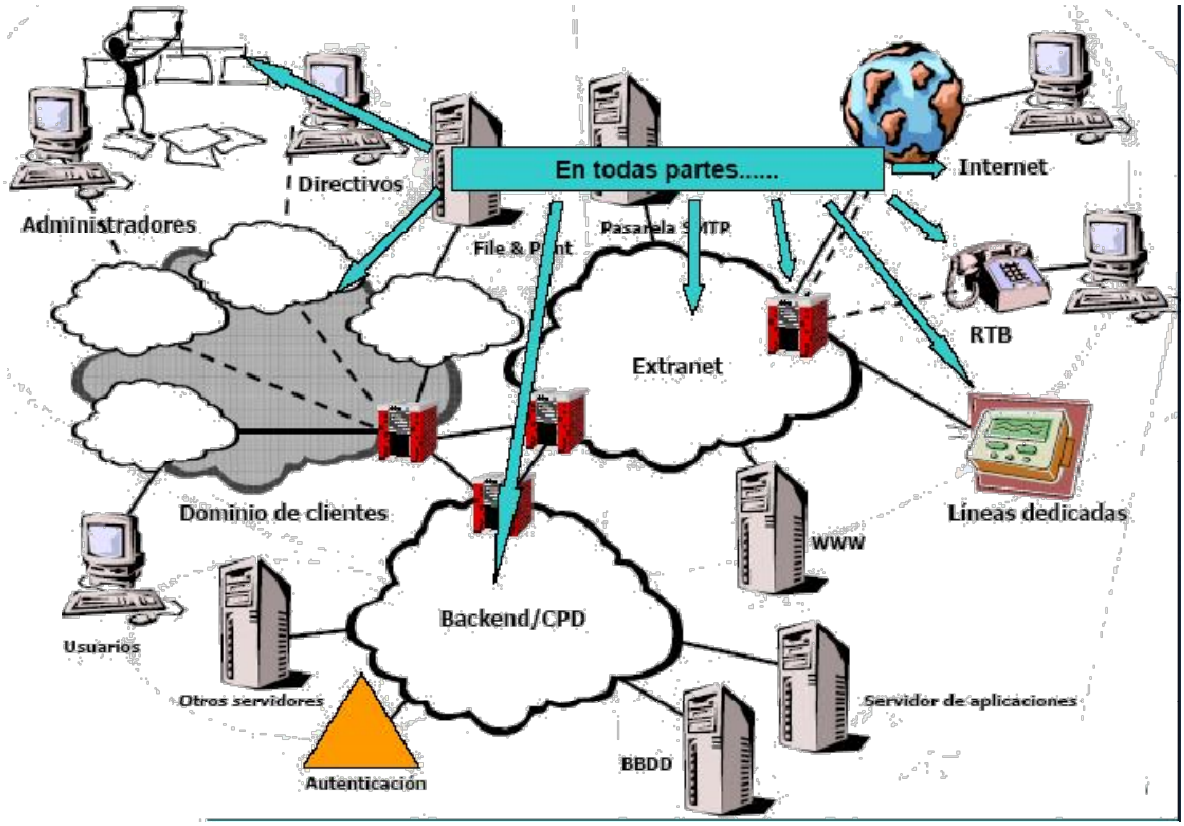
1.3 ¿POR QUÉ ES NECESARIA LA SEGURIDAD DE INFORMACIÓN?

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas de seguridad. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería estar apoyada en una administración y unos procedimientos adecuados. Los controles para la seguridad de la información son considerablemente más baratos y efectivos si se incorporan en la especificación de los requisitos y en la fase de diseño[2]. Además ahí que recalcar y tener presente que la seguridad de información necesariamente debe ser supervisada y controlada de tal forma que se supervise en todo lugar al que se tenga acceso, es decir debe tener control en

[1] ICONTEC, Norma técnica sobre sistema de gestión de seguridad de la información (SGSI), 2005.
[2] Norma Técnica Peruana NTO-ISO/IEC 17799. 2004 p. 10 [Online] Available from World Wide Web: http://bvindecopi.gob.pe/normas/isoiec17799.pdf

todo lugar, desde la intranet hasta la extranet de cada empresa, como lo muestra la figura 1.

Figura 1. Seguridad de Información



Fuente: CORNAGO, Baratech Juan Francisco. Diseño e Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI), según UNE 71502 Dirección de Consultoría.

1.4 REQUISITOS DE SEGURIDAD DE INFORMACIÓN

Los requisitos de la seguridad de la información se deben establecer de tal forma que se cumplan con tres fuentes principales para su establecimiento:

1. Valoración de riesgos de la organización, con ella se identifican las amenazas a los activos, evaluación de vulnerabilidad y probabilidad de ocurrencia, estimación de posible impacto.
2. Requisitos legales, estatutarios, reglamentarios y contractuales que satisfacen la organización, socios comerciales, contratistas y proveedores de servicios.
3. Conjunto de principios, objetivos y requisitos que son parte del procesamiento de la información que la organización desarrolla para apoyar operaciones[3].

1.5 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

Los requisitos para la seguridad de la información se identifican mediante una valoración metódica de los riesgos. La valoración de riesgos es una consideración sistemática de:

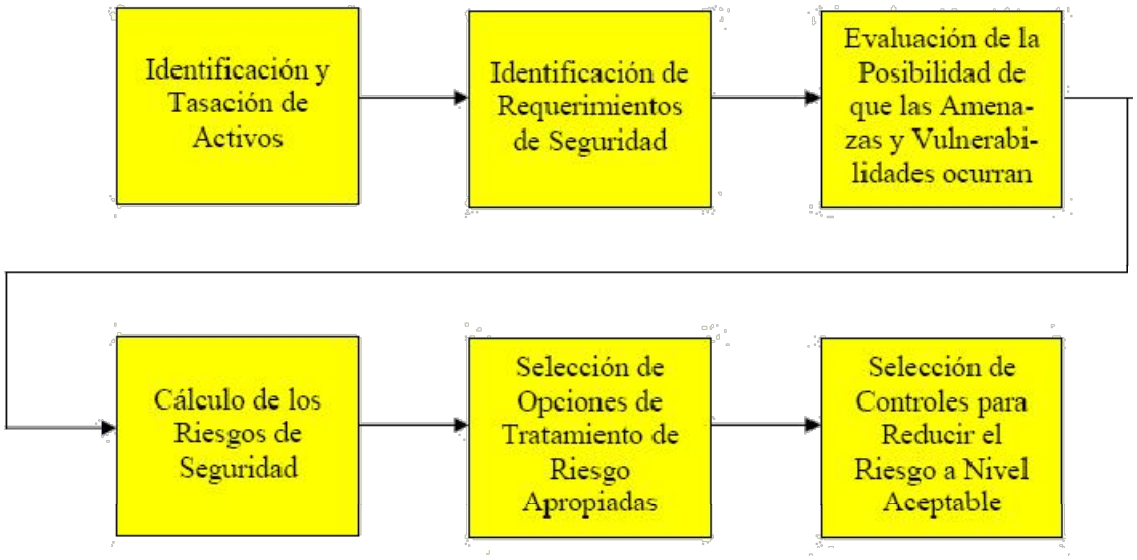
a. La probabilidad de daño al negocio que resulte de una falla de seguridad, teniendo en cuenta consecuencias.
b. De la probabilidad real de que ocurra dicho fallo en consecuencia de las amenazas y vulnerabilidades ya existentes.

Podría requerirse que el proceso de valoración de riesgos y selección de controles se realice varias veces para cubrir las diferentes partes de la organización o sistemas de información individuales, el proceso de evaluación se guía por medio de las revisiones periódicas de los riesgos de seguridad y de los controles implementados como se muestra en la figura 2. De tal forma que se tenga en cuenta los cambios de requisitos y las prioridades del negocio, ya que se puede considerar nuevas amenazas y vulnerabilidades y se confirme que las medidas de

[3] PEÑA, y Lillo Gloria. Gestión de riesgos tecnológicos – UDP, Modulo 6: Mejores prácticas y estándares internacionales en gestión de riesgos y control interno. Diciembre 2005

control siguen siendo efectivas y apropiadas[4].

Figura 2. Proceso de evaluación de riesgo



Fuente: ALEXANDER, Alberto G. Ph,D. CBRP, Auditor SGSI Certificado IRCA. Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El enfoque ISO 27001:2005. [Online] Available from World Wide Web: http://www.centrum.pucp.edu.pe/excelencia

1.6 SELECCIÓN DE CONTROLES DE SEGURIDAD

Una vez se tengan presenten los diferentes riesgos que existen en cuanto a la seguridad de información en una empresa, se empiezan a establecer y seleccionar controles, una vez que se han identificado los requisitos de seguridad. Ciertos controles no son aplicables para todos los sistemas o entornos de información y

[4] ALEXANDER, Alberto G. Ph,D. CBRP, Auditor SGSI Certificado IRCA. Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El enfoque ISO 27001:2005. [Online] Available from World Wide Web: http://www.centrum.pucp.edu.pe/excelencia

puede no ser aplicados en todas las organizaciones. Además los controles se deberían seleccionar con base en su costo de implementación frente a la reducción de los riesgos y pérdidas potenciales si ocurre un incidente de seguridad. También es conveniente tener en cuenta factores no económicos, tales como la perdida de imagen corporativa[5].

1.7 PUNTO DE PARTIDA DE LA SEGURIDAD DE LA INFORMACIÓN

En las empresas por lo general se da la necesidad desde sus inicios empezar a contar con ciertos controles que proporcionen el buen funcionamiento de sus servicios, ciertos controles son un buen punto de partida de la seguridad de la información, estos controles de inicio son referentes al punto de vista legislativo donde se empiezan a considerar controles como son: la protección de los datos y privacidad de la información personal, protección de los registros organizacionales y derechos de la propiedad intelectual, de tal forma que se cumpla con la confiabilidad y el respeto de la información que se tenga de personas o empresas. Además de estos controles se consideran otros como los esenciales para en la práctica seguir con la mejor seguridad de información, estos controles se mencionan a continuación y son esenciales para el buen funcionamiento y eficacia de la empresa:

a. Un documento de la política de seguridad de la información.
b. La asignación de responsabilidades para la seguridad de la información.
c. La educación y formación en seguridad de la información.
d. El reporte de los incidentes de seguridad.
e. La gestión de la continuidad del negocio.

---

[5] Ibíd. Referencia 4.

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos. Un buen punto de partida, no sustituye la selección de controles basada en una evaluación de riesgo[6].

1.8 FACTORES CRÍTICOS PARA EL ÉXITO DE LA SEGURIDAD DE INFORMACIÓN

Los factores críticos de éxito de la implementación de la seguridad de la información de la organización se muestran a continuación:

a. Políticas, objetivos y actividades de seguridad que reflejen los objetivos del negocio.
b. Un enfoque para implementar la seguridad, que sea conciente de la cultura de la organización.
c. El apoyo visible y el compromiso de la alta dirección.
d. Una buena comprensión de los requisitos de la seguridad, de la valoración del riesgo y de la administración del riesgo.
e. Una labor efectiva de concientización acerca de la importancia de la seguridad dirigida a todos los directivos y empleados.
f. La distribución de guías sobre la política de seguridad de la información de la organización y de normas.
g. Formación y capacitación apropiadas.
h. Un sistema de medida completo y balanceado que pueda ser usado para evaluar el desempeño de la administración de la seguridad de la información y la retroalimentación de sugerencias para el mejoramiento[7].

---

[6] Norma Técnica Peruana, NTP-ISO/IEC17799. EDI. Tecnología de Información. Código de Buenas Practicas para la gestión de la Seguridad de la Información. Segunda Edición, Enero 01 de 2007, Lima Perú.
[7] Ibíd. Referencia 6.

2. PROBLEMAS DE SEGURIDAD DE INFORMACIÓN

Existen problemas de seguridad que intervienen en el mal funcionamiento o en la perdida de información ocasionada por actores externos o internos, como son las amenazas activas y las pasivas, caracterizadas principalmente por causar perdidas de datos y perdidas físicas referentes al hardware y software de las máquinas que poseen la información.

2.1 AMENAZAS ACTIVAS

Las amenazas activas hace referencia a un cambio no autorizado y deliberado del estado de un sistema, suponen, de materializarse, la intrusión y posterior interacción con un sistema de información. Ejemplos de amenazas activas son la interrupción, modificación o fabricación de recursos[8].

2.1.1 Gusanos. Programa auto replicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Se propagan a través de la red[9.]

---

[8] A. Ribagorda, Glosario de Términos de Seguridad de las T.I., Ediciones CODA, 1997.

[9] SEGURIDAD EN INTERNET "Programas Maliciosos". [Online] Available from World Wide Web: http://petra.euitio.uniovi.es/~albizu/concursoposter/posters/p3.pdf

2.1.2 Bomba Lógica. Puede ser un programa independiente o un segmento de código:

Evento: El código se activa cuando se cumple alguna condición específica.
Tiempo: Utiliza el reloj del sistema para activarse[10.]

2.1.3 Puertas Trampa. Es un punto de entrada secreto en un programa, de forma que alguien que conozca la existencia de dicha puerta puede obtener permisos de acceso sin tener que pasar por los mecanismos normales de autentificación. La puerta falsa es un código que reconoce alguna secuencia de entrada especial o se dispara si es ejecutado por cierto usuario o por la ocurrencia de una secuencia determinada de sucesos[11.]

2.1.4 Caballo de Troya. Son las amenazas más peligrosas desde el punto de vista de la seguridad, porque una vez instalado el virus en la computadora, los teleoperadores del sistema denominados "crackers" son capaces de manejarla a distancia. Cuando un caballo de Troya esta en el sistema, es posible observar como el cracker, puede leer, modificar, borrar, copiar archivos y programas, de tal manera que el cracker pueda poco a poco eliminar el sistema[12.]

2.1.5 Bacteria. Algunas veces también llamadas conejas, son programas que existen para recuperarse a si mismas, generalmente afectan un sistema por tomar ventaja de los recursos computacionales que ellas consumen solo por existir en el

---

[10] ARGUETA, Amador. Estrategias de Seguridad distribuida en redes bajo ambiente Jini y Java. Capitulo 1: Amenazas en la seguridad en redes. Tesis Licenciatura. Ingeniería de Sistemas Computacionales. Mayo 2001.

[11] STALLINGS, William. Sistemas Operativos, tema 4: Seguridad y Protección. Segunda edición, Madrid. Prentice Hall 1997.

[12] FICARRA, Francisco. Los Virus Informáticos. Chasqui, junio, numero 78. Centro Internacional de Estudios Superiores de Comunicación para América Latina. Quito, Ecuador. 2002

sistema. Mas que propagarse como los virus, las bacterias computacionales simplemente al ser ejecutadas se duplican a si mismas. Las bacterias no alteran los datos ni destruye los archivos, su propósito es degradar el servicio del sistema, pues dependiendo de cómo es programada puede empezar a ocupar todo el espacio del disco muy rápidamente, llevando el sistema a detenerse[13.]

2.1.6 Virus. Programa que tiene la capacidad de modificar otros programas, generalmente introduciendo una copia de si mismo. El programa infectado se usa como vehículo para infectar otros programas. Presenta las siguientes fases:

Propagación: El virus coloca una copia de si mismo en otros programas.
Fase de activación: El virus se activa para realizar la acción para la cual fue construido.
Fase de ejecución: Se realiza la función, esta puede ser inocua (mensaje en pantalla) o dañina (formatear un disco).

Se puede ver que estas amenazas están en el ambiente de la red pública a diario y que muy rara vez la información se salva de ser destruida[14].

2.2 AMENAZAS PASIVAS

2.2.1 Sniffing en Ambiente de Switches. Es posible engañar al protocolo ARP para que una maquina atacante asuma el papel del default gateway, o sea asuma el papel de administrador en este caso de la red y pueda atacar a la red. En este

---

[13] Ibíd. Referencia 12.
[14] MARTINEZ, Juan Carlos. Seguridad en Redes. Diapositivas 7-14 [Online] Available from World Wide Web: http://web.unab.edu.co/~especia/SEG_archivos/frame.htm

caso la maquina atacante reenvía el trafico al verdadero gateway y de esta forma la maquina atacante instala un sniffer y monitorear el trafico[15.]

2.2.2 Sniffing en ambiente de Switches – Macoff. Programa utilizado para enviar a un switch un flujo de direcciones MAC falsas, con el objetivo de saturar la memoria de almacenamiento del switch que esta conectado a una red, de esta forma el switch no podrá almacenar direcciones MAC legítimas. Cualquier nueva trama será enviada por todos los puertos excepto por el puerto en el que se recibió, dando como resultado que el switch se convierte en un hub, luego la actividad de sniffing es posible[16.]

2.2.3 Tempest. Todo equipo electrónico realiza emanaciones eléctricas y magnéticas, el tempest se basa en captar estas emanaciones y de ellas obtener información. Programa establecido en 1950 por el gobierno americano. Tecnología utilizada por agencias gubernamentales[17.]

2.2.4 Ingeniería Social. Este tipo de ataque consiste en engañar a las personas para que colaboren con el atacante, es altamente efectivo y difícil de controlar, ya que es cuestión de persuadir para obtener información de datos para acceder a equipos[18.]

---

15 Ibíd. Referencia 14.
16 Ibíd. Referencia 14.
17 REYES, Clemente Osvaldo. Emisiones Comprometedoras. VIII Seminario Iberoamericano de Seguridad en Tecnologías de Información y Comunicaciones.
18 CARUANA, Pablo. Breves Conceptos sobre la ingeniería Social. Mayo 06 de 2001.

2.2.5 Shoulder Surfing. Requiere de acceso físico, consiste en estar en contacto con las personas a las cuales se les va a hacer el ataque, el contacto para tratar de averiguar contraseñas con las cuales los atacantes puedan acceder tanto al sistema como al servidor, unas de las principales formas de hacer este ataque es tratar de mirar sobre el hombre mientras una persona teclea su contraseña, con el fin de averiguarla ya que algunas personas utilizan la misma contraseña para el protector de pantalla y el servidor[19.]

2.2.6 Estaciones abiertas. Login al inicio del día y logout al final del día, esto consiste en que el usuario de un equipo deja el computador encendido conectado a Internet y deja información a la vista de cualquier intruso, con el fin de tener la posibilidad de acceso no autorizado y envió de e-mail con información critica[20].

2.2.7 Passwords escritas. Escribir la contraseña y tenerla a la mano en caso de olvidarla dejándola en un lugar accesible, es aun mayor el peligro en el caso del administrador del sistema[21.]

2.2.8 Dumpster diving. Escarbar la basura de alguien, algunas compañías no son cuidadosas cuando desechan documentos, computadores etc., la información valiosa de la compañía se puede recuperar.

Estos ataques son hechos por personas que conocen las redes y que están buscando como dañar información de tal forma que actúan como hackers[22].

---

[19] CASTRO, Ospina Sandra Jeannette. "Delitos Informáticos" La información como un bien jurídico y los delitos informáticos en el nuevo código penal Colombiano. Julio 2002. [Online] Available from World Wide Web: http://www.sahw.com

[20] Ibíd. Referencia 14.

[21] Ibíd. Referencia 19.

[22] Ibíd. Referencia 19.

3. SERVICIOS DE SEGURIDAD

Debido al alto índice de perdidas dadas en las empresas se deben implementar servicios de seguridad a través de aplicaciones, protocolos y algoritmos o software de seguridad, por medio de seis servicios de seguridad, que son las claves primordiales para que se asegure la información, estos servicios de seguridad no solo se trata de tecnologías, sino a nivel humano también deben ser aplicados, ya que los trabajadores de empresas deben respetar su entorno de trabajo, y así cuidar la información. Para lo anterior es de gran importancia contar con: Control de acceso, autenticación, privacidad, integridad, no repudio y disponibilidad.

3.1 CARACTERÍSTICAS DE LOS SERVICIO DE SEGURIDAD

Privacidad: La información en un sistema de cómputo y la información transmitida solo es accesible a las entidades autorizadas, de tal forma que ninguna persona ajena a la información pueda observarla y hacer uso indebido de la misma.

Autenticidad: Permite que el origen de un mensaje o documento electrónico sea correctamente identificado, permitiendo a las personas que reciben la información conocer su origen y de esta forma impedir los ataques con virus informáticos.

No repudio: Requiere que las entidades que participan en una comunicación no puedan negar la autoría de un mensaje, permitiendo de esta forma ver la autenticidad del mensaje que se recibe y evitando los ataques de piratas informáticos.

Control de acceso: Requiere que el acceso a los recursos de información del sistema solo se pueda hacer con la debida autorización, por medio de claves.

Disponibilidad: Requiere que los recursos de computo estén disponibles para las entidades autorizadas siempre que se necesite, de tal forma que se genere la buena administración de información.

Es de gran importancia que las personas que trabajan en una empresa estén consientes de la utilidad que tiene la seguridad de la información para la subsistencia del negocio, y es necesario que los encargados de la misma estén atentos a cualquier ataque que se presente en la información[23].

[23] MARAÑON, Álvarez Gonzalo. Servicios de Seguridad. [Online] Available from World Wide Web: http://www.iec.csic.es/criptonomicon/seguridad/servicio.html

4. POLÍTICAS DE SEGURIDAD

Es una declaración formal de reglas que deben ser obedecidas por las personas a quienes se les permite el acceso a la tecnología y a los activos de información de una organización. Una buena política de seguridad muestra a cada empleado en que forma puede contribuir a formar un ambiente seguro. La política debe determinar quien es responsable de determinadas labores como son la construcción, protección, auditoria y revisoría, permitiendo determinar que medidas de contención se van a utilizar. La política determina el "porque", el "como" lo determinan las medidas de contención.

4.1 CARACTERÍSTICAS DE POLÍTICAS DE SEGURIDAD

4.1.1 Accesible. Las políticas que se adecuen en la organización deben responder a ser de conocimiento público dentro de la empresa, puesto que cada persona empleada de la empresa debe conocer que políticas trata la empresa y sus riesgos al incumplirlas. Asimismo debe estar a disposición de los empleados[24].

4.1.2 Definir objetivos de seguridad. Definir porque la seguridad es importante para la organización, con el fin de permitir que al tener políticas en la empresa no se conviertan en innecesarias, además al definir los objetivos de las políticas se

[24] INTERNATIONAL ORGANITATION FOR STANDARDIZATION, Information Technology Code of Practice for Information Security Management. Genera: ISO, 200, 71p. (ISO/IES 17799).

busca que las personas acepten las guías y las pautas que se deben cumplir con el fin de conocer beneficios de política[25].

4.1.3 Definir cada artículo. Al definir la política de seguridad y su objetivo, debe definirse como en toda política de que trata el artículo[26].

4.1.4 Posición de la organización. Definir con lenguaje claro la posición de la organización en cada artículo, de tal manera que se exprese que busca y que quiere de sus empleados para el uso legal de la información. Asimismo deben evitarse párrafos que contengan “inaceptable” y usar palabras como “abuso”, “ofensa”, “legitimo”,”sancionado”, “autorizado”, además se debe justificar cada articulo[27].

---

25 Ibíd. Referencia 24.
26 Ibíd. Referencia 24.
27 Ibíd. Referencia 24.

5. NORMA TÉCNICA SOBRE SISTEMAS DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

En Colombia existen dos normas que permiten la gestión de la información. la norma técnica colombiana NTC-BS 7799-2, esta es la norma que define los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI), mientras que la norma técnica colombiana NTC-ISO/IEC 17799, es el "***Código de buenas practicas para la gestión de la seguridad de la información***", la cual es una guía de todas las políticas y procesos que debe tener una empresa para la gestión de la información.

"La norma NTC-BS 7799-2 viene a cubrir la creciente necesidad de las organizaciones de contar con un adecuado sistema de gestión de la seguridad de la información, sustentado en los controles tecnológicos y organizacionales establecidos en la NTC-ISO/IEC 17799, considerados como las mejores prácticas a nivel internacional. Esto en una economía que depende en forma creciente de los medios tecnológicos, significa una ventaja competitiva notable"[28].

Las experiencias de organizaciones certificadas en otros países permiten identificar algunos beneficios claves de su implementación:

- Reducción de riesgos de seguridad en los procesos de negocio.
- Incremento en la efectividad de las inversiones en controles de seguridad.
- Confiabilidad en las relaciones comerciales a terceros.
- Cumplimiento con regulaciones y requisitos legales.

---

[28] Ibíd. Referencia 1.

6. NORMA TÉCNICA COLOMBIANA NTC-BS 7799-2

"Esta norma ha sido elaborada para los gerentes de organizaciones y su personal, con el objetivo de brindar un modelo para el establecimiento y gestión eficaces de un sistema de gestión de seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos del negocio, los requisitos de seguridad resultantes, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus síntomas de apoyo cambien con el tiempo. Se considera que situaciones simples requieren soluciones de SGSI simples"[29].

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar la eficiencia del SGSI de una organización.

6.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI)

Las empresas que están dedicadas a manejar toda clase de información debe tener claro que en la gestión de la seguridad a nivel de información, es de gran necesidad que se desarrolle, implemente, mantenga y se mejore continuamente un SGSI documentado, en el contexto de las actividades y riesgo del negocio global de la organización, con el fin de que la empresa no tenga el riesgo de perdidas o daños de datos o archivos.

---

[29] Norma Técnica Colombiana NTC-BS 7799-2. Sistema de Gestión de la Seguridad de la Información (SGSI). Requisitos. Diciembre 2004.

Para lo anterior el SGSI, tiene en cuenta los siguientes procesos:

- Establecimiento y Gestión del SGSI.
- Requisitos de documentación.
- Responsabilidades y compromisos de la dirección.
- Gestión de recursos
- Revisión del SGSI por parte de la dirección; que incluye:
- Información para al revisión
- Resultados de la revisión.
- Auditorias internas del SGSI.
- Mejora del SGSI.
- Acciones correctivas.
- Acciones preventivas.

Esto es el fin de promover el buen manejo de información de tal modo que no se presenten pérdidas que dañen la información[30].

6.2 DESARROLLO DE DIRECTRICES PROPIAS DE LOS SGSI

Esta norma se puede ver como un punto de partida para desarrollar una guía especifica para una organización. Las recomendaciones y controles de este código pueden no ser aplicables en su totalidad, incluso pueden requerirse controles adicionales. Cuando esto suceda puede ser útil mantener referencias cruzadas que faciliten la comprobación de la conformidad a los auditores y otros socios del negocio[31].

---

30 Ibíd. Referencia 29.
31 Ibíd. Referencia 29.

7. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 17799

La norma NTC-ISO/IEC 17799, esta basada en la norma Británica BS 7799 en la cual se establecen objetivos de control que aseguran la información para las empresas y que busca que los daños o pérdidas de la misma sea mínima de tal forma que se establezcan políticas y controles que disminuyan el riesgo.

Esta norma aparece para resguardar la creciente necesidad de las organizaciones de contar con un apropiado sistema de gestión de seguridad, reclinado en controles tecnológicos y organizacionales. Asimismo con esta norma lo que se busca es identificar beneficios de disminución de la inseguridad en procesos de negocio, aumento en la efectividad de las inversiones en controles de seguridad, confiabilidad y confidencialidad en relaciones comerciales. De tal forma que se permita generar una significativa ventaja competitiva[32].

7.1 NORMA ISO 17799

"ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada". El objetivo de la seguridad en la información es la de velar por la protección de este activo de tal forma que se asegure la

---

[32] Norma Técnica Sobre Sistemas de Seguridad de la Información (SGSI), NTC-ISO/IEC 17799, 2005.

continuación del negocio, minimizando daños a la organización y maximizando el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de la Confidencialidad, Integridad y Disponibilidad, de tal forma que solo los usuarios autorizados para requerir información puedan manipularla evitando los daños a este activo, y a su ves el objetivo de la norma ISO 17799 se cumpla proporcionando una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad[33].

7.2 ¿A QUIÉN VA DIRIGIDA ISO 17799?

La norma BS 7799 / ISO 17799 puede ser utilizada por cualquier tipo de empresa o de compañía, ya sea privada o pública. Si la organización utiliza sistemas internos o externos que poseen informaciones confidenciales, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información accediéndose a una norma reconocida, la figura 3 muestra los tipos de utilización de la norma de acuerdo al tipo de empresa, su tamaño, su objetivo y la utilización que quieren de la norma[34].

[33] Ibíd. Referencia 6.
[34] Ibíd. Referencia 6.

Figura 3. Clasificación de las Empresas Según Norma ISO 17799

Tipo de empresa	Tamaño	Objetivo principal	Utilización de la norma
Pequeña empresa u organismo	Inferior a 200 empleados	Sensibilizar a la dirección general de la seguridad de la información	La norma ISO 17799 contiene los temas de seguridad que deben tratarse como base de gestión
Empresa media (centralizada o descentralizada)	Inferior a 5000 empleados	Crear una cultura de seguridad global compatible	La norma contiene las prácticas necesarias para constituir una política de seguridad de la información
Empresa muy grande	Superior a 5000 empleadas	Obtener una certificación de seguridad	Utilización de BS7799-2 para crear un documento referencial de seguridad interno

Fuente: PEÑA, y Lillo Gloria. Gestión de riesgos tecnológicos – UDP, Modulo 6: Mejores prácticas y estándares internacionales en gestión de riesgos y control interno. Diciembre 2005

Además de la clasificación de empresas para escoger el tipo de utilización de la norma es de gran necesidad conocer el grado de riesgo del sistema de información que se use, ya que dado el tipo de organización y su objetivo se pueden exponer diferentes grados de utilización de la ISO 17799, en la figura 4 se muestra el grado de exposición de riesgo del sistema de información dependiendo del sector de actividad de la empresa.

Figura 4. Riesgo de Sistema de Información

Fuente: VISON, Jacqueline. La norma BS 7799 / ISO 17799 Para un mejor acercamiento a la seguridad de la información. [Online] Available from World Wide Web: http://www.callio.com

7.3 ESTRUCTURA DE LA NORMA ISO 17799

La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información.

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo[35]. Además la estructura contiene niveles de Seguridad en donde se postran los dominios de control tal y como se muestra en la figura 5.

[35] VILLALON, Antonio. Gestión de Seguridad de Información "La nueva norma UNE 71502. Septiembre 30 de 2004, Valencia. [Online] Available from World Wide Web: http://andercheran.aiind.upv.es/toni/personal/ISO17799.pdf

Figura. 5 Estructura norma ISO 17799

Fuente: Sistemas de Gestión de la Seguridad. ISO 17799 [Online] Available from World Wide Web: http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/curso%2004%2005/presentacion%20ISO%2017799.ppt.

7.3.1 Política de seguridad. Lo que se busca con la política es dirigir y dar soporte a la gestión de la seguridad de la información, la dirección en este caso se debe publicar y comunicar a todos los empleados de forma clara su apoyo a la seguridad de la información, de tal forma que se evite el acceso de virus o cualquier tipo de daño a la información de tal forma que se genere la continuidad del negocio[36].

[36] Ibíd. Referencia 35.

7.3.2 Aspectos organizativos para la seguridad. Se debe gestionar la seguridad de la información dentro de la empresa, en este caso se debe establecer un conjunto de personas que tengan un marco de trabajo para iniciar controlar e implementar la seguridad en la empresa, de tal forma que se asegure el rumbo claro para las iniciativas de seguridad[37].

7.3.3 Clasificación y control de activos. En este caso se debe establecer y hacer un control de los activos físicos y lógicos con los que cuenta la organización de tal forma que se mantenga una protección adecuada sobre los activos de la organización, asegurando un nivel de protección adecuado a los activos de información[38].

7.3.4 Seguridad ligada al personal. De acuerdo a las políticas de seguridad establecidas la empresa o los directivos deben tomar medidas contra las personas no autorizadas que saquen información sin permisos con el fin de reducir los riesgos de errores humanos (robos, fraudes o mal uso de las instalaciones y los servicios), asegurando la disminución de los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos[39].

7.3.5 Seguridad física y del entorno. Se debe evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización, evitando pérdidas, daños[40].

---

37 Ibíd. Referencia 35.
38 Ibíd. Referencia 35.
39 Ibíd. Referencia 35.
40 Ibíd. Referencia 35.

7.3.6 Gestión de comunicaciones y operaciones. Asegurar la operación correcta y segura de los recursos de tratamiento de información, minimizando el riesgo de fallos en los sistemas y protegiendo la integridad del software y de la información. Asimismo se debe mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación, asegurando la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo[41.]

7.3.7 Control de accesos. Lo que se busca en este aspecto es:

- Controlar los accesos a la información.
- Evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo[42].

[41] Ibíd. Referencia 35.
[42] Ibíd. Referencia 35.

7.3.8 Desarrollo y mantenimiento de sistemas. Asegurar que la seguridad está incluida dentro de los sistemas de información, evitando pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones, de tal forma que se proteja la confidencialidad, autenticidad e integridad de la información y así asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura[43.]

7.3.9 Gestión de continuidad del negocio. Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres[44.]

7.3.10 Conformidad con la legislación. Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad, garantizando la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma[45.]

7.4 VENTAJAS DE LA NORMA ISO 17799

"Las organizaciones que hacen uso de la norma ISO 17799 experimentan ventajas competitivas que le permiten garantizar lo siguiente:

- Protección de los bienes de la empresa (información y actividades);
- Protección de la información en las comunicaciones y software;
- Protección ante accesos malintencionados;

---

43 Ibíd. Referencia 35.
44 Ibíd. Referencia 35.
45 Ibíd. Referencia 35.

- Prevención de alteraciones en las comunicaciones entre organizaciones;
- Procesamiento seguro de la información”[46].

7.5 BENEFICIOS DE LA NORMA ISO 17799

Una empresa certificada con la norma técnica ISO 17799 puede ganar frente a sus competidores no certificados. Si un cliente potencial tiene que escoger entre empresas diferentes y la seguridad es un aspecto trascendente, por lo general optará por la certificada. Además una empresa certificada tendrá en cuenta mayor seguridad en la empresa; Planeación y manejo de la seguridad más efectivos; Alianzas comerciales y *e-business* más seguros; Mayor confianza en el cliente; Auditorias de seguridad más precisas y confiables; y Menor responsabilidad civil[47].

A su vez la norma proporciona ventajas que todo buen gerente debería tener en cuenta, en aspectos organizacional, legal, funcional, comercial y financiero. Estos aspectos se mencionan a continuación:

Aspecto organizacional: En este aspecto se adquiere el compromiso de tal forma que se permita garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles y probar la diligencia razonable de sus administradores.

Aspecto legal: En el aspecto legal se establece la conformidad, de tal forma que se permite demostrar a las autoridades competentes que la organización observa todas las leyes y normativas aplicables. En este aspecto, la norma es

---

[46] CASTILLO, Maza Juan, ISO 17799: Gestión de Seguridad de los Sistemas de Información. Ventajas de la norma ISO 17799. 2002 [Online] Available from World Wide Web: http://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/administracion/N10_2003/gesti%C3%B3n.htm

[47] Ibíd. Referencia 46.

complementaria de otras normas y legislaciones ya existentes, por ejemplo: *HIPAA, Privacy Act of 1974, Computer Security Act of 1987, National Infrastructure Act of 1996, Gramm-Leach-Bliley Act of 1999, Government Information Security Reform Act of 2001.*

Aspecto funcional: Hace referencia a la gestión de los riesgos, en la obtención de un mejor conocimiento de los sistemas de información, sus fallas y los medios de protección. Garantiza también una mejor disponibilidad de los materiales y datos, de tal forma que no se pierda información ni que esta este a disposición de pérdidas o daños.

Aspecto comercial: En este aspecto se genera la Credibilidad y confianza, de tal forma que los socios, los accionistas y los clientes se tranquilicen al constatar la importancia que la organización concede a la protección de la información.
Una certificación también puede brindar una diferenciación sobre la competencia y en el mercado. Algunas licitaciones internacionales ya comienzan a pedir una gestión ISO 17799.

Aspecto financiero: Reducción de los costos vinculados a los incidentes y posibilidad de disminución de las primas de seguro.

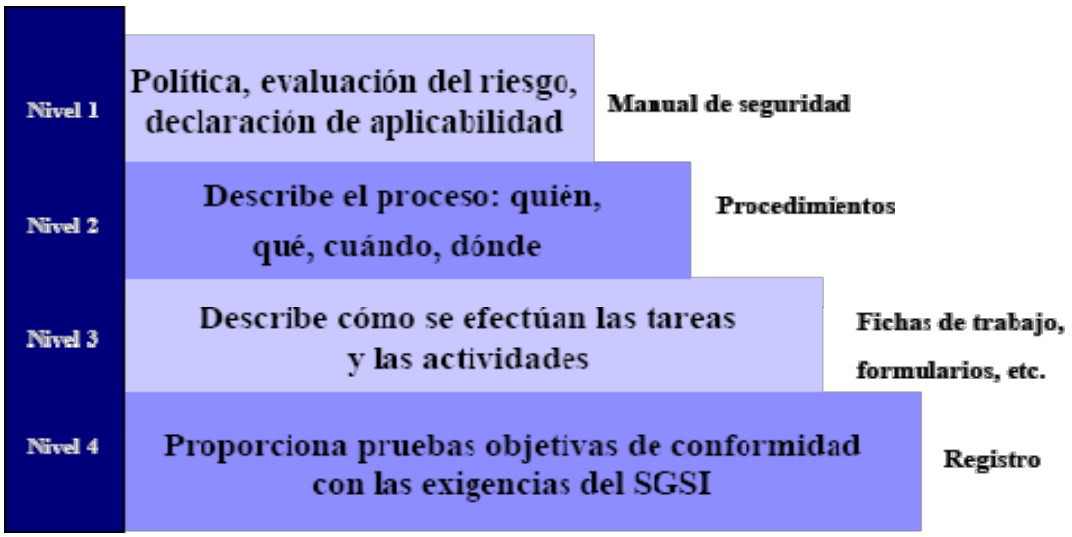
Aspecto humano: Mejora la sensibilización del personal a la seguridad y a sus responsabilidades en la organización.

7.6 DOCUMENTACIÓN DE UN SGSI

La documentación de un SGSI es una exigencia importante de la implantación y se articula en torno a dos ejes:

1. La descripción de la estrategia del organismo, sus objetivos, la evaluación de riesgos y las medidas tomadas para atenuarlos.
2. El control y el seguimiento del funcionamiento del SGSI. Existen por lo menos cuatro niveles de documentación como se muestra a continuación:

Figura 6. Niveles de Documentación SGSI



Fuente: VISON, Jacqueline. La norma BS 7799 / ISO 17799 Para un mejor acercamiento a la seguridad de la información. [Online] Available from World Wide Web: http://www.callio.com

7.6.1 Obstáculos de Documentación SGSI. Al encontrarnos con la habilidad del SGSI para traer cambios en las organizaciones, se puede ver que existen algunos obstáculos en su implantación, algunos de estos a saber son los siguientes:

- Temor, resistencia a los cambios.
- Riesgo de que los cambios realizados en un área requieran ajustes en otras áreas.
- Aumento de los costos.
- Insuficiente conocimiento del enfoque utilizado

- Tareas que parecen insuperables.

Debido a lo anterior es de gran necesidad ayudar a superar estos obstáculos es por esto que se deben considerar algunos factores de éxito para dar a entender que la implantación de SGSI no es mala[48].

7.6.2 Factores de éxito. La experiencia ha probado que los factores enumerados a continuación son a menudo cruciales para garantizar el éxito de la implementación de gestión de la seguridad de la información en una organización.

a. Una política, objetivos y actividades de seguridad en el que reflejan los objetivos de la empresa.
b. Una puesta en ejecución de la gestión de la seguridad que sea compatible con la cultura de la organización.
c. Un apoyo y compromiso visibles de la dirección.
d. Una buena comprensión de las exigencias de seguridad, de la evaluación de los riesgos y de la gestión de los riesgos.
e. Una presentación eficaz de las cuestiones de seguridad a todos los responsables y empleados.
f. La distribución a todos los empleados y a todos los proveedores de las directrices sobre la política y las normas de seguridad de la información.
g. Una formación y una educación conveniente.
h. Un sistema de medidas completo y equilibrado utilizado para evaluar la eficacia de la gestión de la seguridad de la información y la aplicación de los requerimientos de mejoras resultantes de dicha evaluación[49].

---

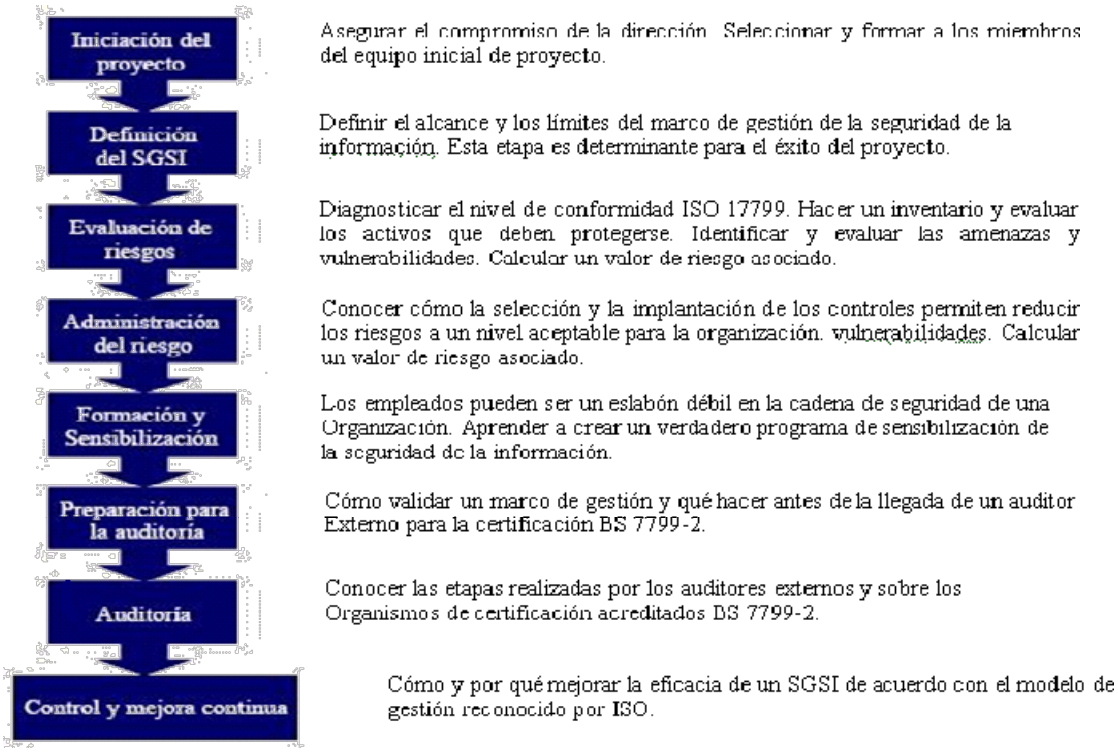
[48] Ibíd. Referencia 46.

[49] BRUNA. Ignacio-Polin. Una Administración Efectiva de la Seguridad de la Información. 2004. [Online] Available from World Wide Web: http://www.belt.es/articulos/articulo.asp?id=1439

7.7 IMPLEMENTACIÓN DE UN SGSI

El gráfico siguiente describe cada una de las ocho etapas de implantación de un SGSI:

Figura 7. Etapas implementación SGSI



Fuente: ALVAREZ. José Alfonso. Desarrollo de una metodología para desarrollo e implementación de las tecnologías y sistemas de Información. [Online] Available from World Wide Web: http://www. Fca.uach.mx/posgrado/diseño%20de%20una%20metodologia%20para%20desarrollo.pdf

8. PROTOTIPO GEICO “SISTEMA DE GESTIÓN DE SEGURIDAD BASADO EN ISO 17799”

8.1 ARQUITECTURA Y DISEÑO DEL PROTOTIPO

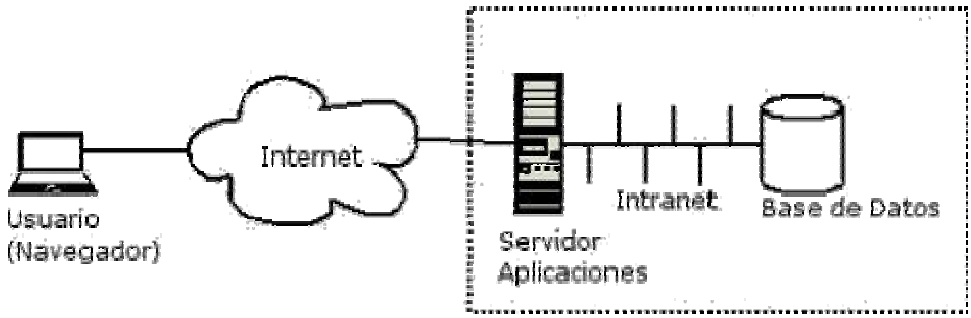
Teniendo en cuenta que los diferentes sistemas de información basados en la norma ISO 17799 creados hasta la actualidad han sido hechos para ser accesibles por Internet, utilizando aplicaciones Web, las cuales se han convertido en interfaces de sistemas complejos lo mas parecidas a las aplicaciones de escritorio dando confianza a los usuarios al momento de interactuar con el sistema. Por lo anterior el prototipo GEICO (Gestión, Implementación y Control) que se construyó, utiliza aplicaciones Web con el propósito de cumplir con ciertas necesidades, entre las cuales esta que la información sea compartida entre las partes interesadas, de manera que todas tengan acceso a la información completa o aquella parte que les corresponda según su función en cada momento, a su ves se busca que la información sea accesible desde cualquier lugar dentro de la organización e incluso desde el exterior para el encargado de realizar de solicitar el servicio del prototipo de Gestión de Seguridad desarrollado.

La aplicación Web utilizan el modelo o arquitectura de tres capas, en donde, el usuario interactúa con las aplicaciones Web a través del navegador. Como consecuencia de la actividad del usuario, se envían peticiones al servidor, donde se aloja la aplicación y que normalmente hace uso de una base de datos que almacena toda la información relacionada con la misma.

El servidor procesa la petición o las preguntas existentes en la aplicación y devuelve la respuesta al navegador que es el encargado de presentarlas al

usuario, de tal forma que el servidor muestre una serie de solicitudes hechas a la Web, en este caso controles que se deben implementar de acuerdo a la cantidad de respuestas negativas o positivas que se contesten en una serie de formularios que el usuario debe diligenciar. Por tanto, el sistema se distribuye en tres componentes: el navegador, que representa la interfaz de usuario; la aplicación, que se encarga de realizar las operaciones necesarias según las acciones llevadas a cabo por este y la base de datos, donde la información relacionada con la aplicación, como se aprecia en la figura 8.

Figura 8. Arquitectura de Tres Capas



Fuente: CASTEJON, Garrido Juan Salvador. Arquitectura y diseño de sistemas web modernos. Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia [Online] Available from World Wide Web: http://www.cii-murcia.es/informas/ene05/articulos/Arquitectura_y_disenyo_de_sistemas_web_modernos.html

En la mayoría de los casos, el navegador suele ser solo un presentador de información, y no lleva a cabo ningún procesamiento relacionado con la lógica de negocio.

En el prototipo construido, utiliza un patrón de diseño o un esqueleto de las soluciones a problemas comunes en el desarrollo del software que se divide en tres niveles:

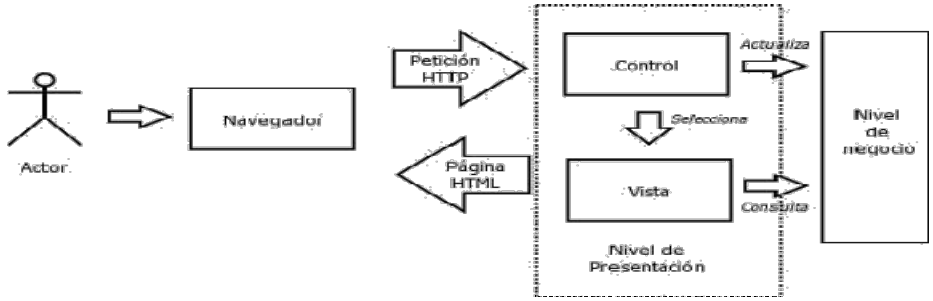
- **Nivel de presentación**: es el encargado de generar la interfaz de usuario en función de las acciones llevadas a cabo por el mismo.

- **Nivel de negocio**: contiene toda la lógica que modela los procesos de negocio y es donde se realiza todo el procesamiento necesario para atender a las peticiones del usuario.

- **Nivel de administración de datos**: encargado de hacer persistente toda la información, suministra y almacena información para el nivel de negocio.

8.1.1 Arquitectura MVC (Modelo/Vista/Control). Además de que la aplicación presente arquitectura de tres capas como se describió en el numeral 9.1, este prototipo tiene un patrón Web Modelo-Vista-Control (MVC), conocida también como arquitectura MVC. Este patrón propone la separación en distintos componentes de la interfaz de usuario (vistas), el modelo de negocio y la lógica de control, como se observa en la figura 9. Una vista es una "fotografía" del modelo (o una parte del mismo) en un determinado momento. Un control recibe un evento disparado por el usuario a través de la interfaz, accede al modelo de manera adecuada a la acción realizada, y presenta en una nueva vista el resultado de dicha acción. Por su parte, el modelo consiste en el conjunto de objetos que modelan los procesos de negocio que se realizan a través del sistema.

Figura 9. Patrón de Diseño MVC



Fuente: CASTEJON, Garrido Juan Salvador. Arquitectura y diseño de sistemas web modernos. Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia [Online] Available from World Wide Web: http://www.cii-murcia.es/informas/ene05/articulos/Arquitectura_y_disenyo_de_sistemas_web_modernos.html

El modelo presenta arquitectura presenta varias ventajas:

- Hay una clara separación entre los componentes de un programa; lo cual nos permite implementarlos por separado.
- Hay un API, la cual hace referencia a un conjunto de especificaciones de comunicación entre componentes del software muy bien definido; cualquiera que use el API, podrá reemplazar el Modelo, la Vista o el Controlador, sin aparente dificultad.
- La conexión entre el Modelo y sus Vistas es dinámica; se produce en tiempo de ejecución, no en tiempo de compilación.

Al incorporar el modelo de arquitectura MVC al diseño desarrollado, se pudo observar que las piezas de un programa se pueden construir por separado y luego unirlas en tiempo de ejecución. Si uno de los Componentes, posteriormente, se observa que funciona mal, puede reemplazarse sin que las otras piezas se vean afectadas.

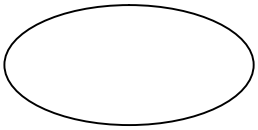
8.2 ANÁLISIS

8.2.1 Modelo Funcional. El cual modela los diferentes servicios que ofrecerá el prototipo, utilizando para este modelamiento los diagramas de casos de usos representando la interacción dinámica que tienen acabo el actor usuario (administrador WEB, Administrador Usuario, Usuario normal), y el actor sistema con el prototipo, con el fin de desarrollar la aplicación mas fácilmente sin que se perdieran requerimientos de cada actor del sistema.

8.2.1.1 Casos de Uso. Un caso de uso es una descripción de un conjunto de secuencias de acciones que un actor ejecuta y que produce un resultado observable de interés para un actor particular. Un caso de uso se utiliza para estructurar los aspectos de comportamiento en un modelo, en el anexo A se puede apreciar el diagrama con los casos de uso del usuario, relacionados con el prototipo GEICO. Estos casos de uso que se desarrollaron tienen como finalidad mostrar más detalladamente lo que debe hacer tanto el sistema como el usuario para que las peticiones lleguen a recibir una respuesta.

Gráficamente, un caso de uso se representa como una elipse de borde continuo, incluyendo normalmente sólo su nombre[50], como se muestra a continuación.

Figura 10. Casos De Uso



Fuente: SCHMULLER, Joseph. Aprendiendo UML en 24 horas, México. Editorial Pearson Education 2000.

[50] BOOCH, Grady. El lenguaje de Modelado Unificado. Madrid. Editorial Addison Wesley, 1999.

Los casos de uso están conformados por varios componentes:

Actor: Es una entidad externa al sistema que se modela y que puede interactuar con él. Un actor representa un conjunto coherente de roles que los usuarios de los casos de uso juegan al interactuar con estos. Normalmente, un actor representa un rol de una persona, un dispositivo hardware o incluso otro sistema al interactuar con un sistema.[51]

Relaciones: Es una conexión entre los elementos del modelo. Las relaciones entre casos de uso y actores pueden ser las siguientes:

- Un actor se comunica con un caso de uso.
- Un caso de uso extiende otro caso de uso.
- Un caso de uso usa otro caso de uso.

Los diagramas de caso de uso se utilizan para el modelamiento de aspectos dinámicos del sistema, subsistema o clase. Se emplean para modelar la vista estática de casos de uso de un sistema. Son importantes para visualizar, especificar y documentar el comportamiento de un elemento[52].

Para abordar un análisis completo en la elaboración del prototipo de sistema de recomendación, los requerimientos del actor usuario es un factor muy importante para la construcción de un buen prototipo, en GEICO (Gestión, Implementación y Control), dichos requerimientos son:

- Registrarse en el Sistema.

---

[51] ERIKSSON, Hans-Erik and PENKER, Magnus. "UML Toolkit" Wiley Computer Publishing [online] Available from World Wide Web: http://www.fi-b.unam.mx/pp/profesores/carlos/aydoo/toc.html

[52] Ibíd. Referencia 59.

- Enviar los respectivos formularios que se presentan al registrarse y al acceder como usuario administrador.
- El usuario administrador puede acceder a información de la norma ISO 17799 y a un glosario de la norma.

Al prototipo (GEICO “sistema de gestión de seguridad basado en la norma ISO 17799”) realizado, se le ha configurado un actor administrador, quien a su vez como el actor usuario, presenta ciertos requerimientos que contribuirán en la construcción del sistema, dichos requerimientos son:

- Obtener los mismos beneficios de un actor usuario
- Permitir o no, ciertas beneficios a ciertos usuarios.
- Responder los formularios de recopilación de información, con el fin de acceder a los cuestionaros de auditoria para evaluar la seguridad
- Solicitar pagina, lo cual se hace después de registrarse en el sistema

Además de el usuario administrador, se ha configurado un usuario Administrador WEB, quienes son los encargados de toda la parte administrativa de la pagina y sus bases de datos, este actor tiene las siguientes tareas representadas de una forma mas completa en el **ANEXO A,** donde aparecerán los casos de uso:

- Administrar página, que tiene diferentes casos incluidos los que son: Buscar, Agregar y Modificar página.
- Administrar la base de datos, que al igual que el caso de uso anterior se busca, agrega y modifica, además de esto se elimina.
- Administrar usuario, que tiene casos de uso incluidos como buscar, agregar, modificar y eliminar.

8.3 DISEÑO DEL PROTOTIPO

Para esta etapa de diseño se tomaron los requerimientos y el modelado de la etapa de análisis. Para esta etapa, se desarrollan cinco procedimientos necesarios para la elaboración de un buen diseño.

8.3.1 Diseño de Base de Datos. Teniendo el modelo entidad relación, se lleva a cabo la transformación en un diseño de base de datos. Para la selección del diseño de la base de datos, se debe tener en cuenta las tareas y la complejidad de las búsquedas y consultas.

Existen cinco tipos principales de base de datos: simple o plana, red, jerárquica, relacional y orientada a objetos. Se ha escogido como base de datos para la elaboración del prototipo, la relacional; permitiendo la utilización de relaciones entre distintos conjuntos de información para generar consultas complejas.

8.3.2 Documentación de los casos de uso. La documentación de los casos de uso, es realizada en base a la plantilla, la cual permite hacer una secuencia de todas las actividades que realiza un caso de uso en particular dichas actividades.

En el **ANEXO B**, se puede apreciar la documentación de los casos de usos mas relevantes del prototipo GEICO ”sistema de gestión de seguridad basado en la ISO 17799”, como los casos de uso del actor usuario, actor administrador de la WEB. Estando entre los requerimientos del actor administrador, “obtener los mismos beneficios de un actor usuario” la lista de eventos son similares, a excepción de los eventos “Preparación de auditorias” “recopilación de Información”

y “solicitar pagina”, adicionando a su lista de casos de uso, eventos propios de un actor administrador del sistema.

8.3.3 Diseño de Eventos. Haciendo uso de la herramienta UML (Lenguaje de Modelado Unificado), se hace mas fácil el diseño de los diagramas de interacción de los eventos propios del prototipo, ya que elaborando como primera instancia el diagrama de secuencia se puede apreciar cómo es el desarrollo interno de cada caso de uso, referente a el actor que los solicite.

En segunda instancia, basándonos en los diagramas de secuencia se pueden construir los diagramas de colaboración, mostrando el orden de ejecución de las relaciones, llamados de clases o tablas (dado el caso que se presente) entre las clases, relaciones y objetos propio de cada caso de uso.

Finalmente, teniendo todos los diagramas de secuencia necesarios para la elaboración de un buen diseño de eventos del prototipo, se realiza la construcción del diagrama de clases, la cual encierra todas las clases, interfaces y relaciones de todos los diagramas de colaboración.

8.3.3.1 Diagrama de Secuencia. Es un tipo de diagrama de interacción. Muestran las interacciones entre un conjunto de objetos. En los diagramas de este tipo intervienen objetos, que tienen un significado parecido al de los objetos representados en los diagramas de colaboración, es decir son instancias concretas de una clase que participa en la interacción. El objeto puede existir sólo durante la ejecución de la interacción.

Un diagrama de secuencia representa una forma de indicar el período durante el cual un objeto está desarrollando una acción directamente o a través de un procedimiento.

Los diagramas de secuencia permiten indicar cuál es el momento en el que se envía o se completa un mensaje mediante el tiempo de transición, que se especifica en el diagrama.

8.3.3.2 Diagrama de Colaboración. Muestra la interacción entre varios objetos y los enlaces que existen entre ellos. Representa las interacciones entre objetos organizadas alrededor de los objetos y sus vinculaciones. A diferencia de un diagrama de secuencia, un diagrama de colaboraciones muestra las relaciones entre los objetos, no la secuencia en el tiempo en que se producen los mensajes

Los diagramas de secuencia y los diagramas de colaboraciones expresan información similar, pero en una forma diferente. Durante la ejecución de un diagrama se crean y destruyen objetos y enlaces.

Los diagramas de secuencia y colaboración derivados de los casos de uso en general, se pueden apreciar en el **Anexo C**.

8.4 CONSTRUCCIÓN

Con base a los visto en el numeral 8.1 se ha decidido aplicar la arquitectura MVC, para el desarrollo de las aplicaciones Web. En base al diagrama de clases modelado en la etapa de diseño, puede representar la arquitectura MVC del prototipo.

8.4.1 Herramientas de Desarrollo. La aplicación del prototipo se ejecutará sobre un esquema Web, teniendo como herramientas de desarrollo:

- Software contenedor WEB. Para este caso se usará la herramienta APACHE.
- Software motor de BD. Para este caso se usará la herramienta **MySQL4.1 Database Server de MySQL AB**.
- Desarrollo de Interfaces. Para este caso se usara la herramienta PHP 4.0

8.5 DESCRIPCIÓN DE PANTALLAS

8.5.1 Pantalla Principal. Esta pantalla contiene el menú del sistema, el cual tiene unos ítems de opción dependiendo de la persona que ingrese al sistema; usuario normal o administrador.

En el caso de Usuario normal, se muestra una barra con el menú del sistema, que contiene opciones como:

- Registrar
- Ver información de la norma
- Ver glosario
- Solicitar Pagina

En el caso del administrador, por ser un usuario con privilegios posee las mismas opciones del manejo hacia el sistema que el usuario normal, contando con otras opciones referentes a la administración del sistema. Las actividades de este usuario son:

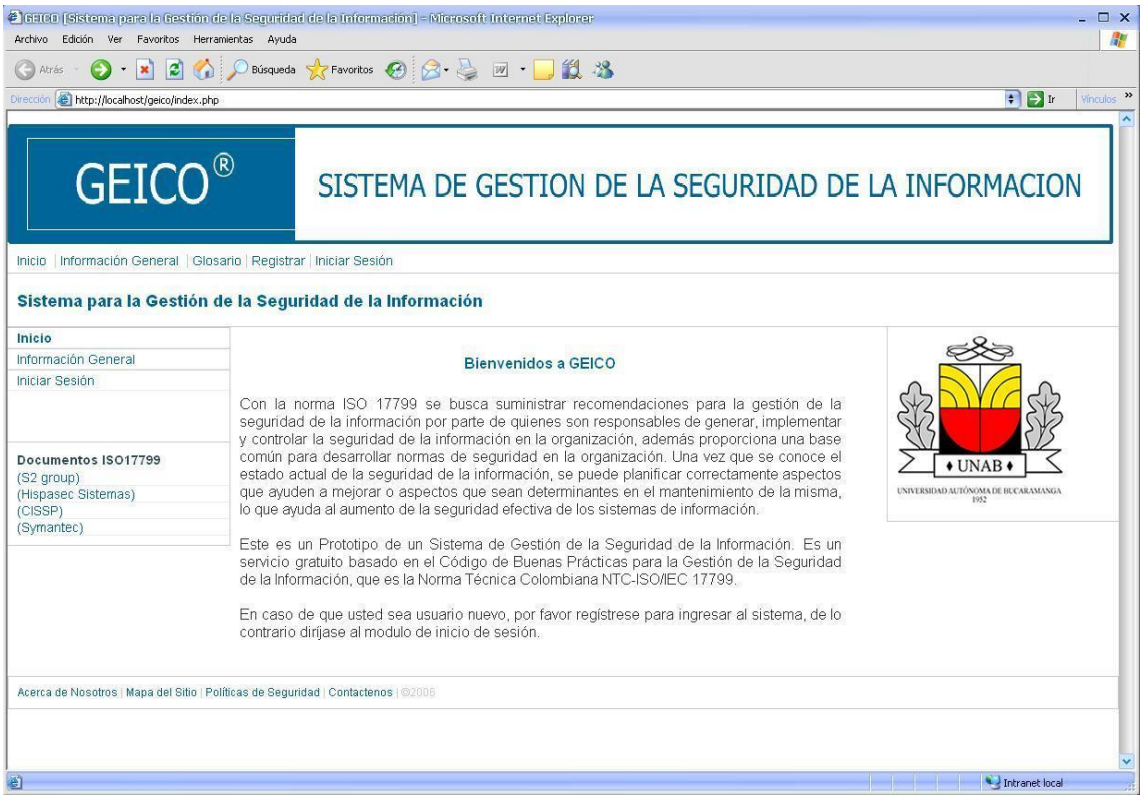
- Registrarse

- Preparación de auditorias
- Diagnostico SGSI
- Recopilación de Información
- Evaluar cuestionarios

Por ultimo tenemos al actor Administrador de Web, quien va a realizar sus eventos desde la misma página, estos eventos son:

- Publicar Web
- Administrar pagina, Base de Datos y Administrar Usuario

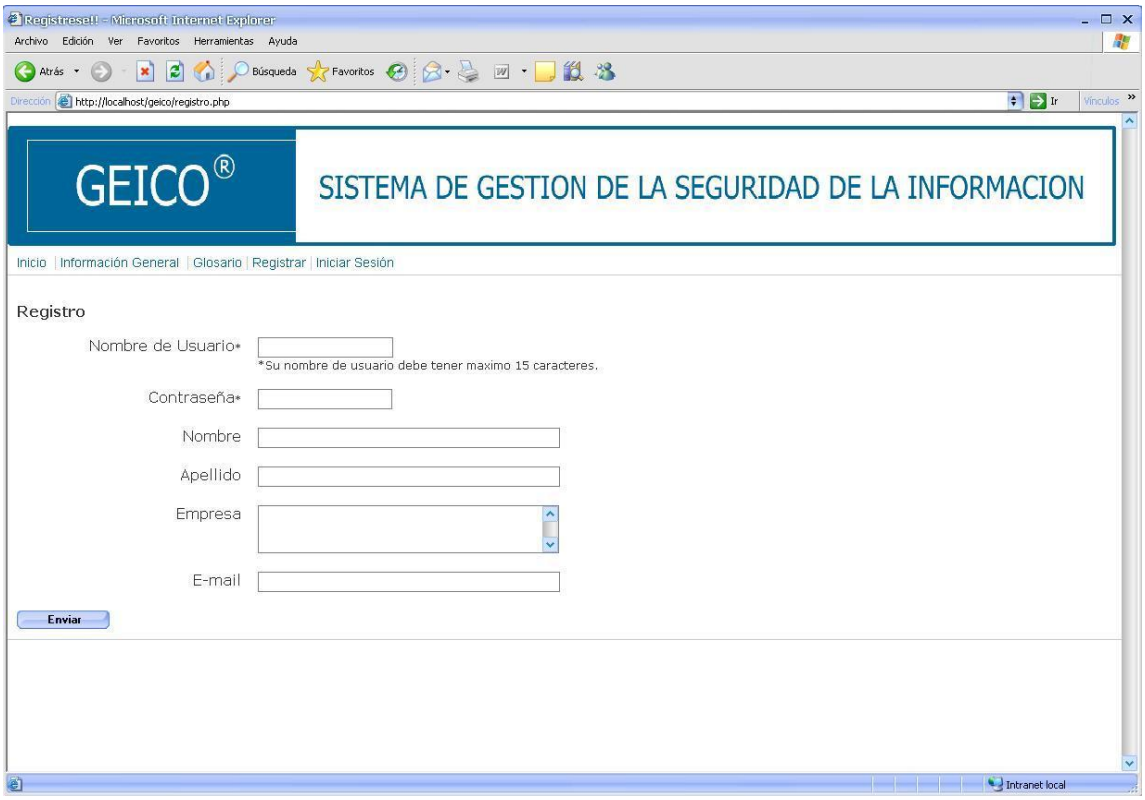
Figura 11. Inicio del prototipo



Fuente: Autores del Proyecto

8.5.2 Registro de Usuario. Interfaz a la que se tiene acceso en caso que el usuario no se haya registrado en el sistema, y se desea pertenecer a el, o si es el caso de algún usuario ya registrado y desea realizar una actualización en la información que dio en el momento de registrarse en el sistema como vez primera, en este caso puede acceder a esta pantalla, seleccionando la opción registrar de la barra de menú. Este evento se muestra en la figura 12.

Figura 12. Evento Registro en Sistema

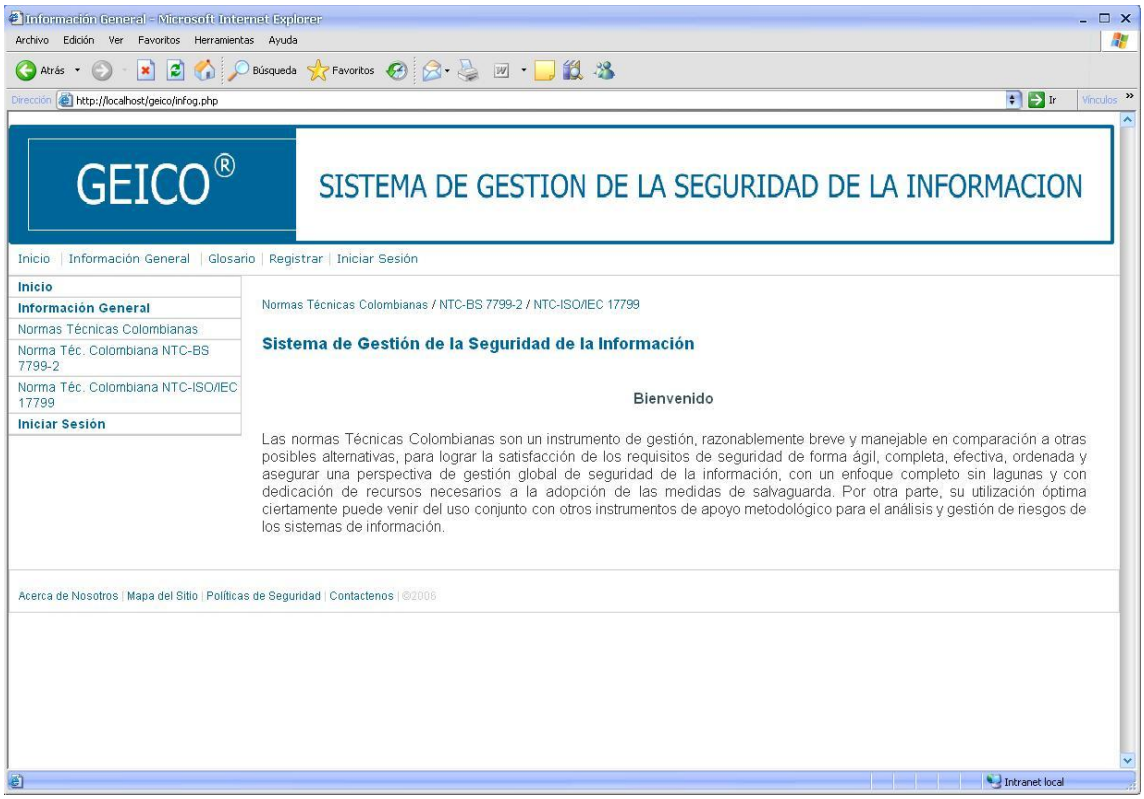


Fuente: Autores del Proyecto

8.5.3 Información General. A través de esta interfaz el usuario ya sea con privilegios o sin ellos puede acceder a información de la norma y del sistema, de

tal forma que pueda interactuar con la información de la Web. En este caso se presenta información de la norma en la página y en archivos tipo PDF.

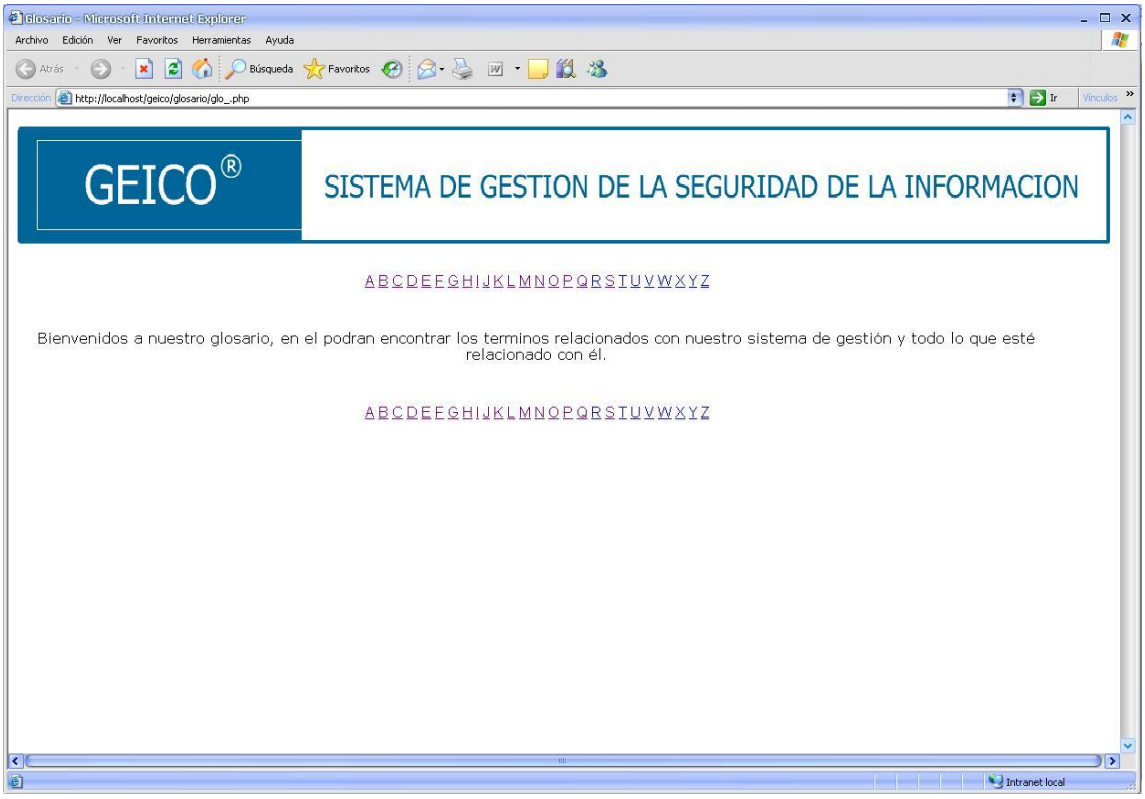
Figura 13. Evento Ver Información del Sistema



Fuente: Autores del Proyecto

8.5.4 Glosario. A través de esta interfaz el usuario puede acceder a la información de algunas palabras que no tienen significados claros para los usuarios.

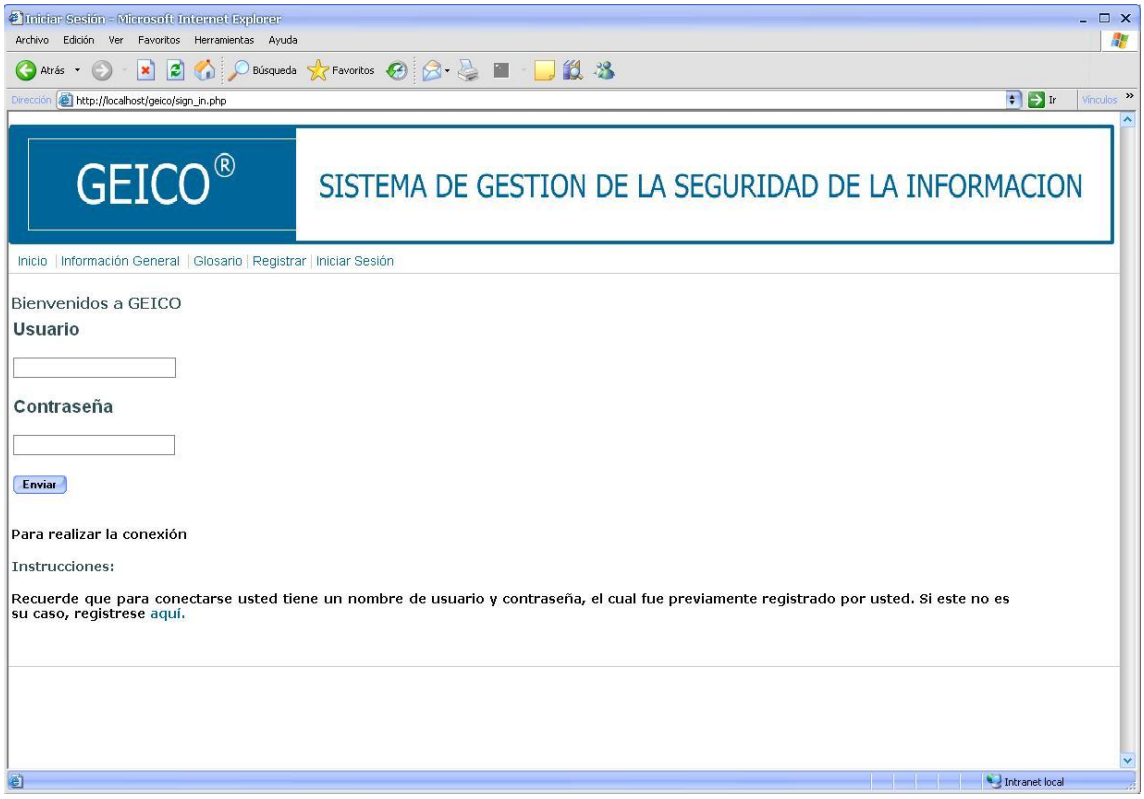
Figura 14. Evento Ver Glosario



Fuente: Autores del Proyecto

8.5.5 Ingresar al sistema (INICIO). En la interfaz por donde ingresa tanto el usuario como el administrador del sistema, para que dicho ingreso sea exitoso, se deberá escribir mediante el teclado el login y password de acceso, o se puede acceder sin ser administrador para acceder solo a información de la norma, en este caso no se cuenta con privilegios.

Figura 15. Inicio de Sesión



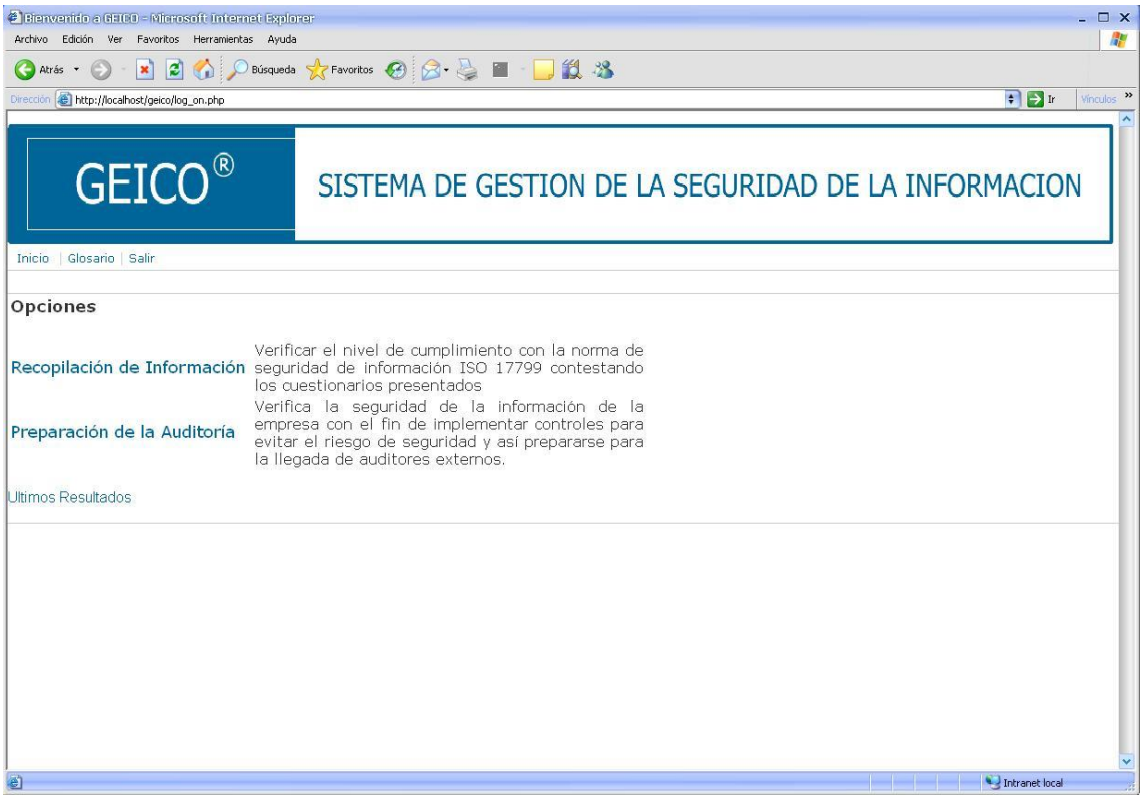
Fuente: Autores del Proyecto

8.5.6 Inicio. Luego de ingresar a la página de conexión y de digitar datos de usuario y contraseña el usuario accede a un vínculo donde se le muestra una bienvenida y dos opciones “Recopilación de Información” y “Preparación de Auditoria”, en cualquiera de estos dos casos el usuario debe estar registrado. Esta Interfase se puede ver en la figura 16.

8.5.7 Recopilación de Información. En la interfaz que en primera instancia se debe ejecutar es la interfaz 16 Donde se muestran dos opciones “Recopilaron de Información” y “Preparación de Auditoria”, en este momento como el evento que

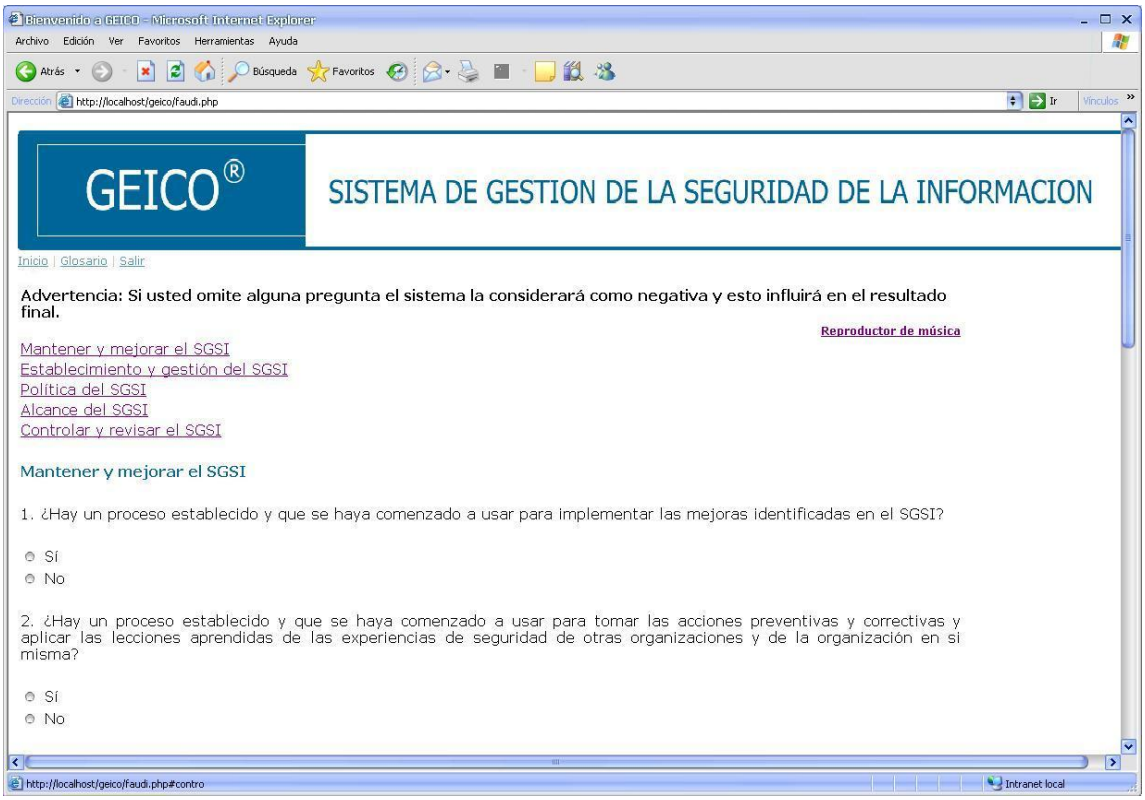
se va a mostrar es Recopilación de Información, al darle clic en este ítem, se despliega la interfaz mostrada en la figura 17:

Figura 16. Eventos Recopilación Información y Preparación de Auditorias



Fuente: Autores del Proyecto

Figura 17. Evento Recopilación de Información



Fuente: Autores del Proyecto

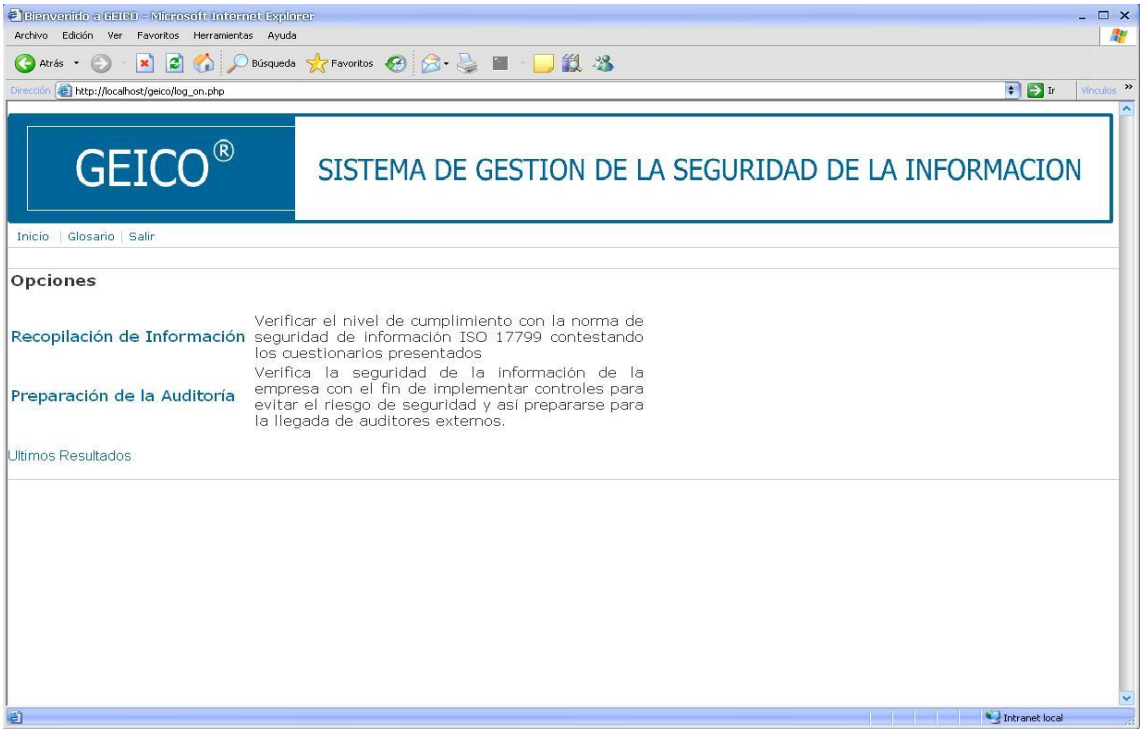
La interfase “Recopilación de Información”, muestra un formulario el cual debe evaluar el interesado en utilizar el prototipo, este evento se realiza con el fin de recopilar información del estado actual de la empresa con referencia a la seguridad de la información.

8.5.8 Preparación de Auditorias. En esta pantalla se muestra el ítem que tiene la auditoria de tal forma que se pueda acceder al formulario que se quiera de acuerdo a lo que el usuario decida evaluar, en este caso se muestran 10 opciones que son:

- Políticas de Seguridad
- Seguridad física y del entorno y del personal
- Administración de la continuidad del negocio
- Clasificación y control de activos
- Control de acceso y cumplimiento
- Desarrollo y mantenimiento de sistemas
- Gestión de comunicación y operaciones
- Organización de la seguridad.

La interfase que se puede observar al querer ejecutar este evento, como primera instancia es la que presenta la opción “Preparación de Auditorias”, como se muestrea en la figura 18.

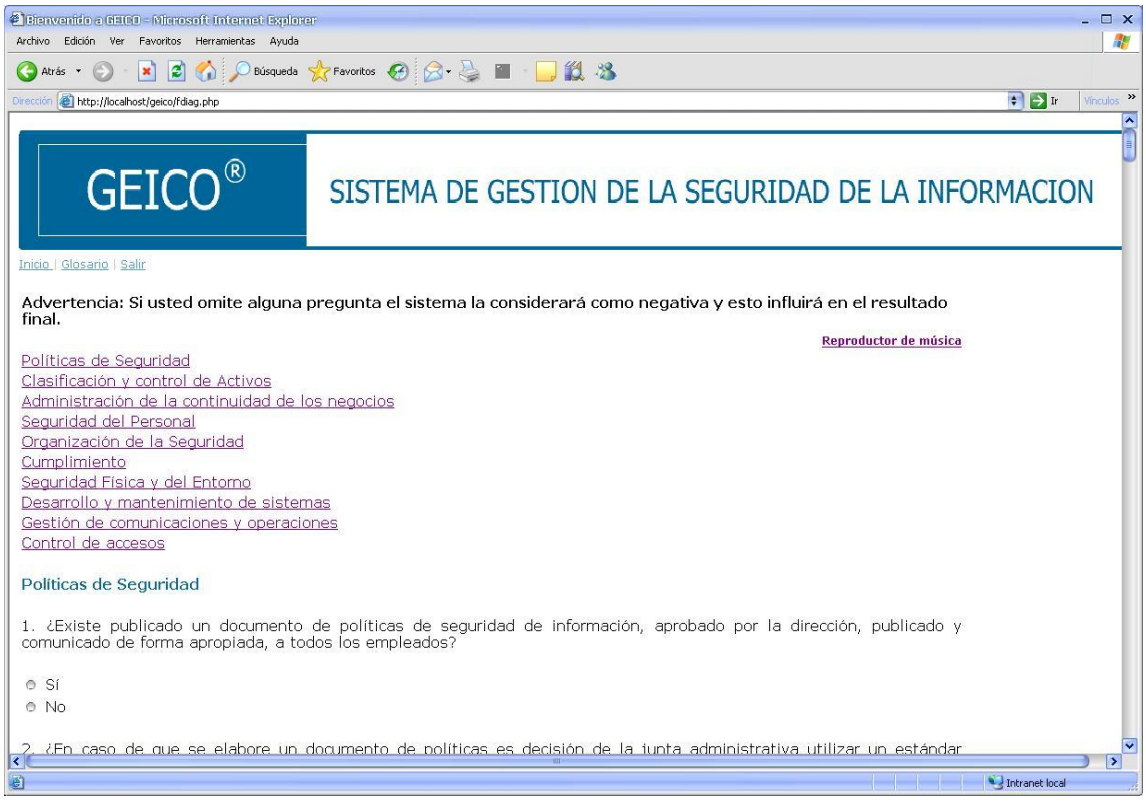
Figura 18. Eventos Recopilación Información y Preparación de Auditorias



Fuente: Autores del Proyecto

Si el usuario accede al evento Preparación de Auditoria, se despliega una pantalla como la que se muestra en la figura 19, donde nos muestra las opciones que anteriormente se mencionaron.

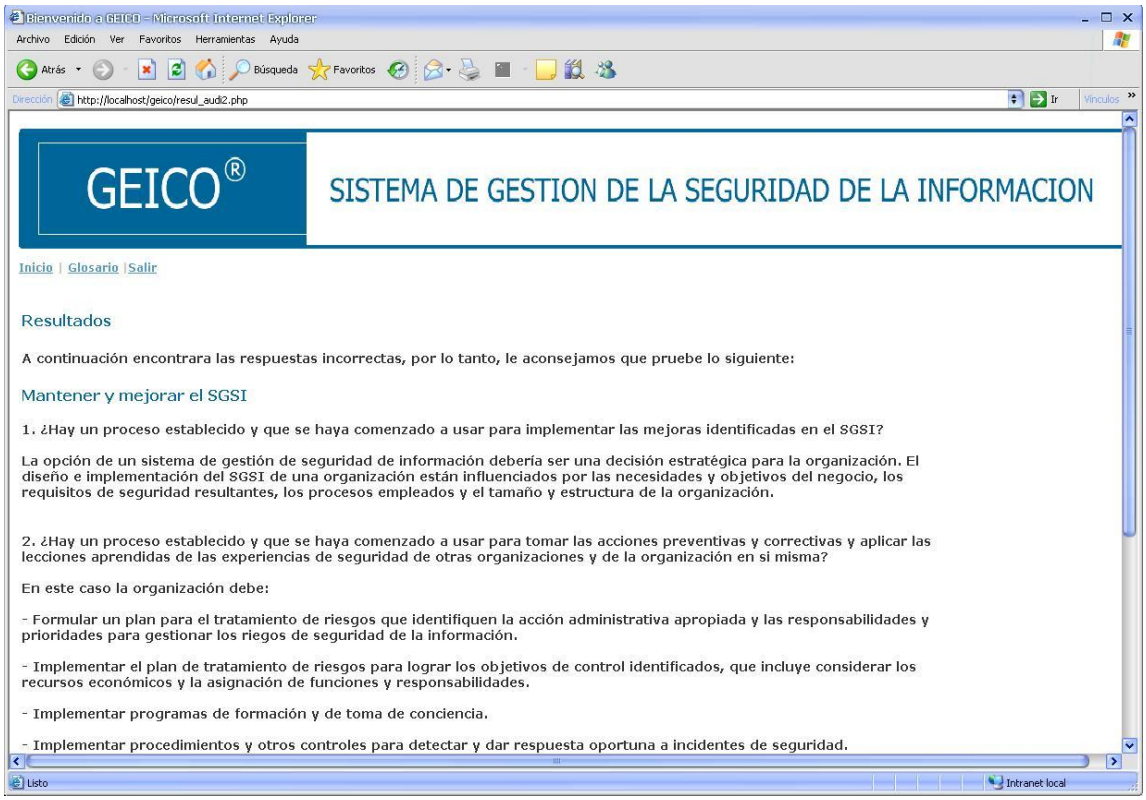
Figura 19. Auditoria



Fuente: Autores del Proyecto

Después de haber realizado la evaluación de auditoria de acuerdo a los ítems que se seleccionaron, el sistema muestra una interfase con los resultados de la auditoria donde se les dan tips a los usuarios para mejorar la seguridad de información. Esta interfase se ve en la figura 20.

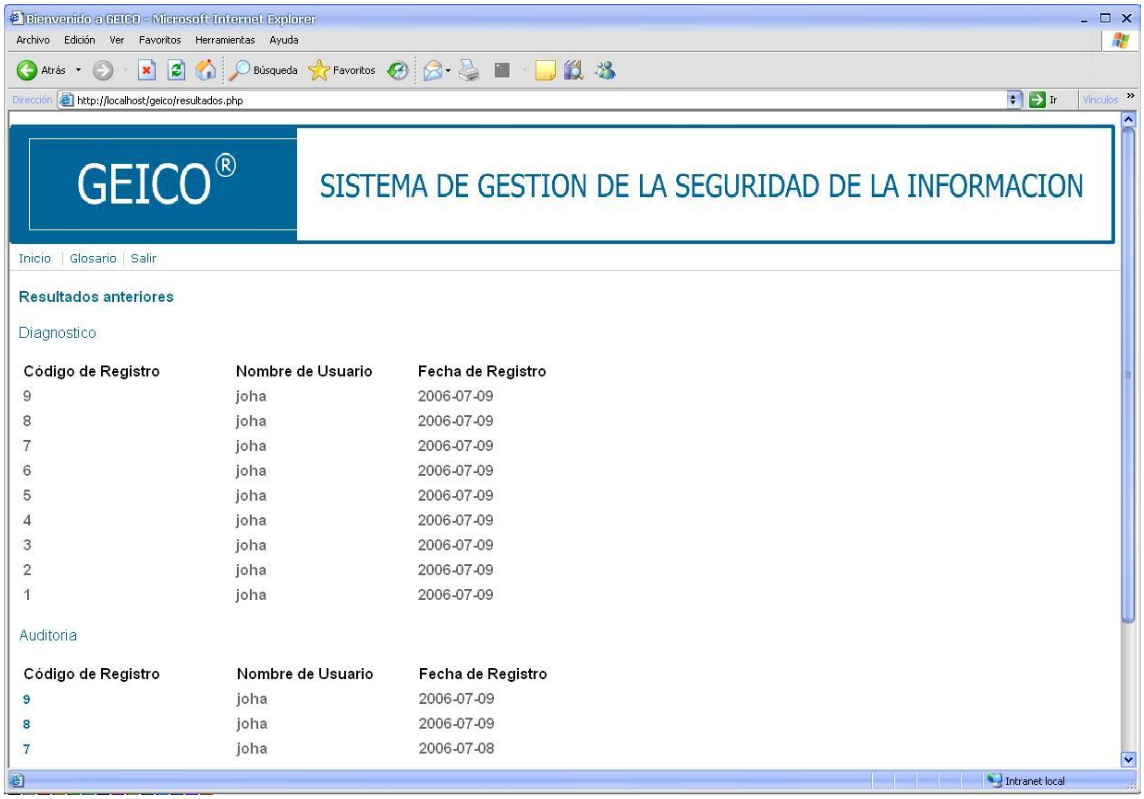
Figura 20. Resultados de Auditoria



Fuente: Autores del Proyecto

8.5.9 Registro de evaluación por usuario. En esta pantalla se presentan los registros que tiene cada usuario que ha evaluado los formularios de Auditoria y recopilación de Información, con el fin de que cada vez que se decida evaluar la seguridad de Información, el usuario pueda observar si continua o no cometiendo fallas para la protección de la información

Figura 21. Registro de Evaluación por Usuario



Fuente: Autores del Proyecto

9. CONCLUSIONES

La elaboración del prototipo GEICO basada en la norma ISO 17799 es de gran ayuda para las empresas ya que sin necesidad de que las personas estén en contacto con un libro pueden verificar que tan buena es la seguridad de información en las empresas, con este prototipo las empresas tienen un proceso adecuado para aplicar Sistemas de Seguridad de Información, pues la aplicación inicia con la evaluación actual de la organización y posteriormente identifica los cambios que se necesitan para cumplir con la norma para así dar las mejores recomendaciones para realizar la gestión de la seguridad de la información. Además ISO 17799 propicia las bases para promover acciones de tipo preventivo.

Al abordar temas como la seguridad de información es de gran necesidad conocer que es la seguridad, las clases de amenazas que existen, con el fin de incorporar medidas de prevención en las tecnologías de información, ya que en la sociedad que vivimos la información constituye el mas grande capital de las empresas y organizaciones, y su administración no tendrá valor si la seguridad no es privada y exclusiva.

BIBLIOGRAFÍA

PERDITA, Stevens Rob Pooley. “Utilización de UML en Ingeniería de Software con Objetos y Componentes”. Addison Wesley 2002.

SCHMULLER, Joseph. Aprendiendo UML en 24 horas. México. Editorial Pearson Education 2000. 423 páginas.

BOOCH, Grady. EL lenguaje de Modelado Unificado, Madrid. Editorial Addison Wesley 1999. 432 páginas.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Code of Practice for information Security Management. Genev: ISO, 200, 71p. (ISO/IEC 17799)

BRITISH STANDARDS INSTITUTION. Information Security Management Systems. Specification with Guidance for Use. London, BSI. pp 33 (BS 7799-2:2002).

STALLINGS, William. Sistemas Operativos, Segunda Edición, Madrid. Editorial Prentice Hall. 707 páginas.

ICONTEC, Norma técnica sobre sistema de gestión de seguridad de la información (SGSI), NTC-ISO/IEC 17799. 2005.

ICONTEC, Norma técnica sobre sistema de gestión de seguridad de la información (SGSI), 2005.

CORNAGO, Baratech Juan Francisco. Diseño e Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI), según UNE 71502 Dirección de Consultoría.

PEÑA, y Lillo Gloria. Gestión de riesgos tecnológicos – UDP, Modulo 6: Mejores prácticas y estándares internacionales en gestión de riesgos y control interno. Diciembre 2005

ARGUETA, Amador. Estrategias de Seguridad distribuida en redes bajo ambiente Jini y Java. Capitulo 1: Amenazas en la seguridad en redes. Tesis Licenciatura. Ingeniería de Sistemas Computacionales. Mayo 2001.

REYES, Clemente Osvaldo. Emisiones Comprometedoras. VIII Seminario Iberoamericano de Seguridad en Tecnologías de Información y Comunicaciones.
CARUANA, Pablo. Breves Conceptos sobre la ingeniería Social. Mayo 06 de 2001.

VISÓN, Jacquelin, CISSP Analista en Seguridad de Información, Callio Technologies Rene Saint-Germain, Presidente, Callio Technologies. La norma BS

7799/ISO 17799, para un mejor acercamiento al a seguridad de la información. Documento de presentación. [Online]. Disponible en Internet http://www.callio.com. Fecha de consulta 20 febrero 2006

VILLALÓN, Antonio. Código de Buenas practicas de seguridad UNE-ISO /IEC 17799. [Online]. Publicado el 30 Septiembre 2005. Disponible en Internet http://andercheran.aiind.upv.es/toni/personal/ISO17799.pdf . Fecha de consulta 15 febrero 2006

VILLALON, Antonio. Gestión de Seguridad de Información "La nueva norma UNE 71502. 30 de Septiembre 2004 Valencia. [online]. Disponible en http://andercheran.aiind.upv.es/toni/personal/ISO17799.pdf. Fecha de consulta 15 febrero 2006

ÁLVAREZ, José Alfonso. Desarrollo de una metodología para desarrollo e implementación de las tecnologías y sistemas de información [online]. Publicado en Agosto 2005. Disponible en Internet http://www.fca.uach.mx/posgrado/diseno%20de%20una%20metodologia%20para%20desarrollo.pdf . Fecha de consulta 25 enero 2006

SEGURIDAD EN INTERNET "Programas Maliciosos". [Online] http://petra.euitio.uniovi.es/~albizu/concursoposter/posters/p3.pdf Fecha de consulta 10 mayo 2006

FICARRA, Francisco. Los Virus Informáticos. Chasqui, junio, numero 78. Centro Internacional de Estudios Superiores de Comunicación para América Latina. Quito, Ecuador. 2002 Fecha de consulta 10 mayo 2006

CASTRO, Ospina Sandra Jeannette. “Delitos Informáticos” La información como un bien jurídico y los delitos informáticos en el nuevo código penal Colombiano. Julio 2002. [Online] http://www.sahw.com. Fecha de consulta 10 mayo 2006

MARAÑON, Álvarez Gonzalo. Servicios de Seguridad. [Online] http://www.iec.csic.es/criptonomicon/seguridad/servicio.html Fecha de consulta 12 mayo 2006

ALEXANDER, Alberto G. Ph,D. CBRP, Auditor SGSI Certificado IRCA. Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El enfoque ISO 27001:2005. [Online] http://www.centrum.pucp.edu.pe/excelencia Fecha de consulta 15 febrero 2006

CASTEJON, Garrido Juan Salvador. Arquitectura y diseño de sistemas web modernos. Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia [Online] Disponible en internet: http://www.cii-murcia.es/informas/ene05/articulos/Arquitectura_y_disenyo_de_sistemas_web_modernos.html. Fecha de consulta 15 marzo 2006.

MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [online]. Disponible en Internet http://www.csi.map.es/csi/pg5m20.htm. Fecha de consulta 01 marzo 2006

Software de conformidad BS7799 / ISO17799 en español [online]. Disponible en Internet http://www.callio.com/es/ . Fecha de consulta 5 de enero 2006

ISO TS 17799**.** Sector Normas IT & Ebusiness [online] Disponible en http://www.bvqiarg.com.ar/certificaciones/ISO17799.html . Fecha de consulta 17 de febrero 2006

ETEK International Holding Corp [online]. Disponible en Internet http://www.etek.com.co/. Fecha de consulta 15 febrero 2006

Internet Solutions [online]. Disponible en Internet http://www.internet-solutions.com.co. Fecha de consulta 15 febrero 2006

GALINDO, John, Gerente de DIGIWARE S.A., Soluciones de Seguridad informática. [Online] Disponible en Internet www.digiware.com.co. Fecha de consulta 17 febrero 2006

Norma Técnica Peruana NTO-ISO/IEC 17799. 2004 p. 10 [Online]. Disponible en Internet http://bvindecopi.gob.pe/normas/isoiec17799.pdf. Fecha de consulta 14 marzo 2006

MARTINEZ, Juan Carlos. Seguridad en Redes. Diapositivas 7-14 [Online]. Disponible en Internet http://web.unab.edu.co/~especia/SEG_archivos/frame.htm Fecha de consulta 10 mayo 2006

CASTILLO Maza, Juan, ISO 17799: Gestión de seguridad de los sistemas de información. Ventajas de la norma ISO 17799. 2002. [Online] Disponible en Internet http://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/administracion/N10_2003/gesti%C3%B3n.htm Fecha de consulta 14 marzo 2006

BRUNA, Ignacio-Polin. Una administración efectiva de la seguridad de la información. Publicado 09 enero 2004. [Online]. Disponible en Internet http://www.belt.es/articulos/articulo.asp?id=1439. Fecha de consulta 14 marzo 2006]:

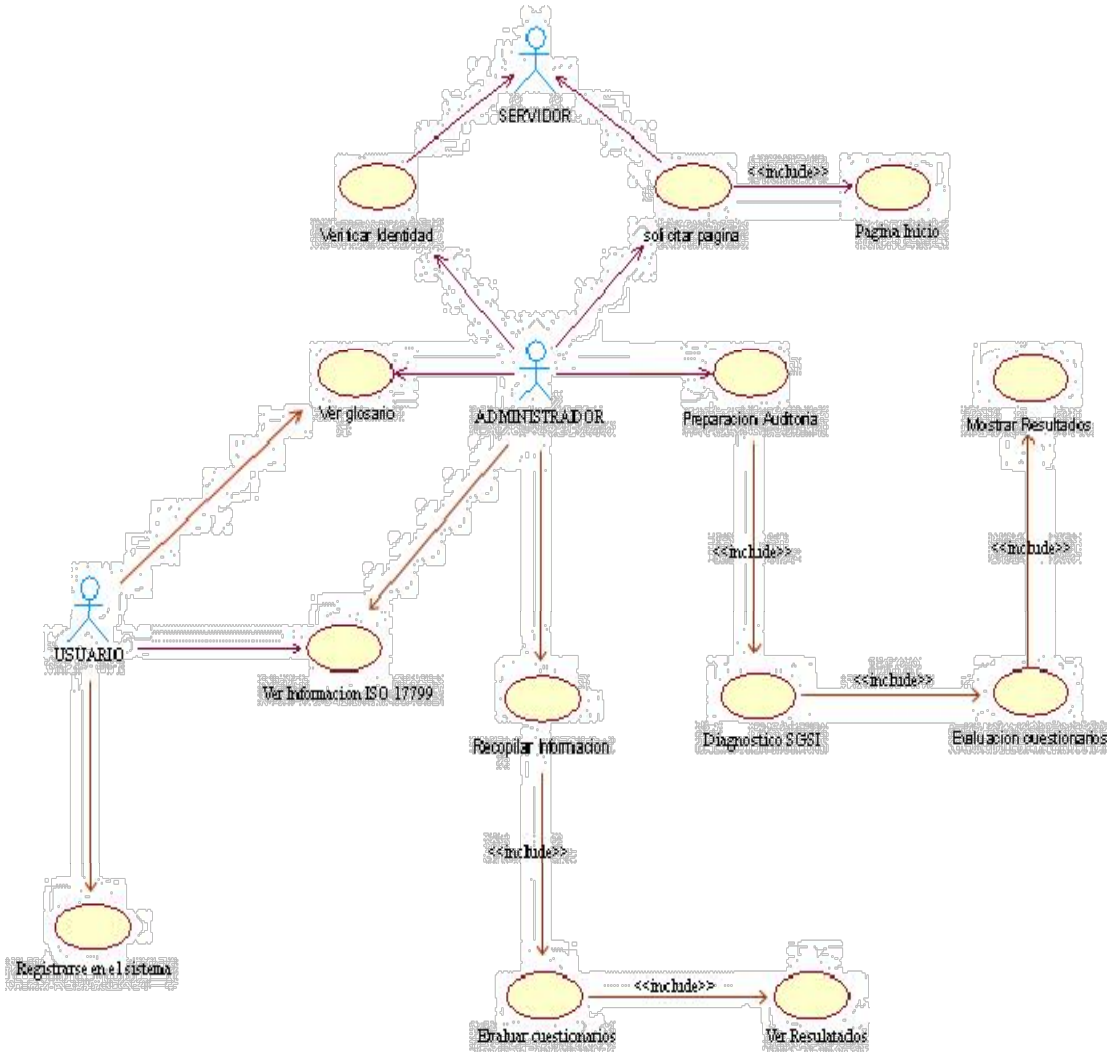
PEREDA, Fernando J. y CERVERA NAVARRO, Ricardo. Introducción a PHP. [online]. http://www.ferdyx.org/charlas/intro_php/charla-simo.pdf Fecha de consulta 10 diciembre 2005

Software de conformidad BS7799 / ISO17799 en español. [Online] http://www.callio.com/es/ . Fecha de consulta 20 febrero 2006,

ANEXOS

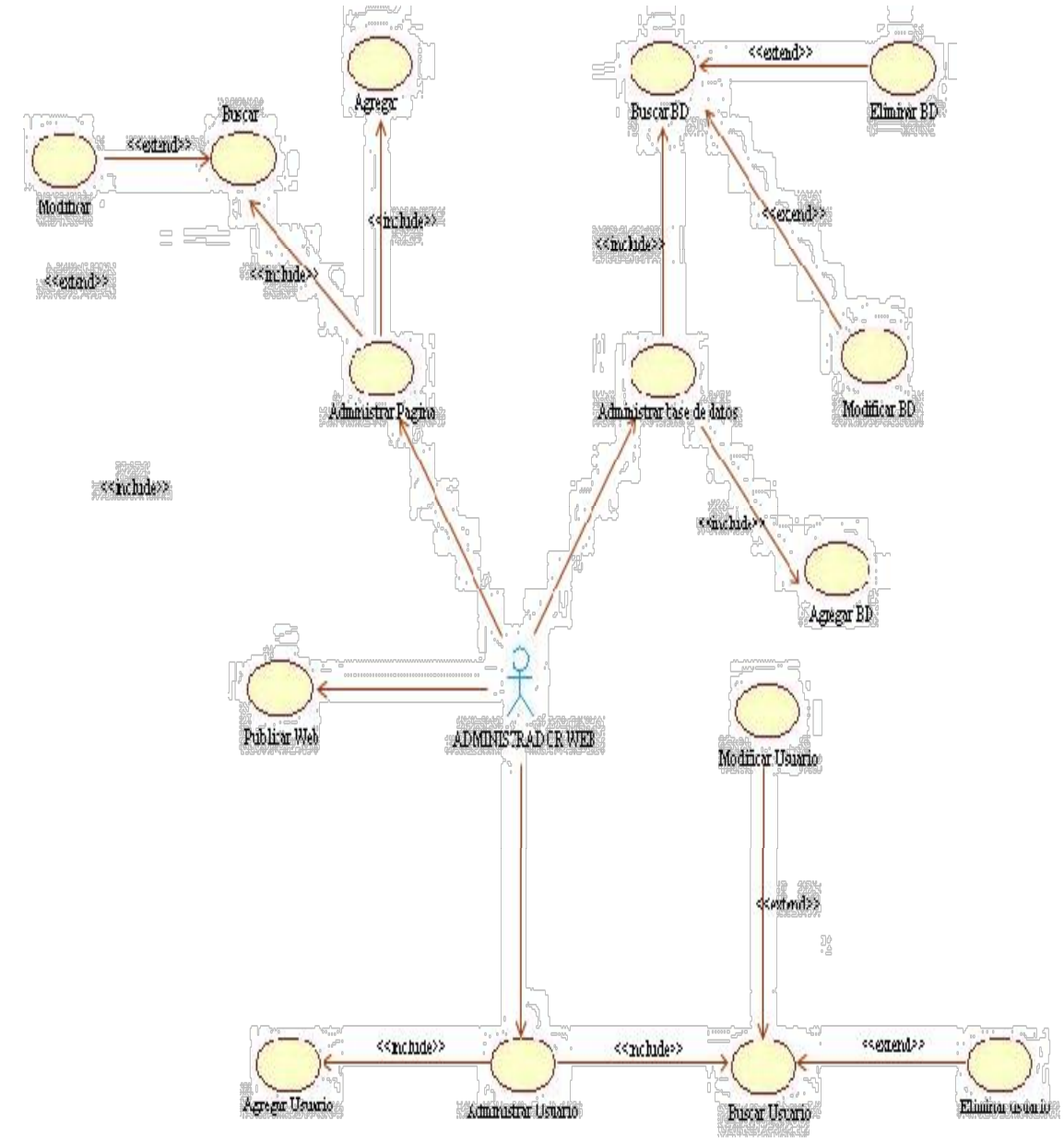
Anexo A. Diagrama de caso de uso

Figura 22. Diagrama De Caso De Uso Usuario - Administrador



Fuente: Autores del Proyecto

Figura 23. Diagrama de Caso de Uso Administrador Web



Fuente: Autores del Proyecto

Anexo B. Documentación casos de uso

La documentación de los casos de uso, se realizan para los actores Usuario y Administrador, ya que estos son los que interactúan directamente con la aplicación, al igual que los diagramas de secuencia y colaboración que se presentan en el **ANEXO C**.

ACTOR ADMINISTRADOR

EVENTO: RECOPILACIÓN DE INFORMACIÓN

1. DESCRIPCIÓN

El usuario al acceder a inicio en la pantalla principal, puede acceder a privilegios y convertirse en usuario administrador, en este caso el usuario tiene la opción de acceder a un evento “Recopilación de Información”, este caso de uso permite al usuario evaluar formularios o cuestionarios de tal forma que al responder a cada pregunta, esta se va guardando en la base de datos, se validan las respuestas de acuerdo a un SI o NO y se finaliza mostrando unos resultados.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- El usuario accede a la ventana de identificación o ítem inicio
- Ingresa el login y password
- El login y password ingresados son validos
- Se autoriza el ingreso al menú principal
- Seleccionar recopilación de información
- Muestra cuestionarios
- Responde cuestionarios

2.2 FLUJO DE EVENTOS

Si alguno de los datos ingresados no son validos, el sistema devuelve la misma interfaz en espera de ingresar los datos validos.

El Usuario debe responder las preguntas de los cuestionarios, ya sea con un si o no, en caso que se desee salir de este evento la base de datos guarda la información ya expuesta.

3. REQUERIMIENTOS ESPECIALES

El usuario debe estar registrado con un login y un password

4. POSCONDICIONES

El usuario puede acceder a el evento Preparación de auditorias

ACTOR USUARIO

EVENTO: REGISTRARSE EN EL SISTEMA

1. DESCRIPCIÓN

El este evento, un usuario accede a la pagina inicio, al usuario se le muestra la opción registro, luego el sistema muestra un formulario, donde se digitan los datos de usuario, este formulario tiene como contenido; el nombre de usuario, password, confirmación de contraseña, nombre, apellido, empresa y por último correo electrónico o e-mail

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- El usuario selecciona una opción para registrarse en el sistema.
- Se genera una ventana para que el usuario se registre.

- El usuario llena los campos solicitados por el sistema, que son necesarios para la creación de un nuevo registro de usuario. Mínimo deben ser llenados los campos de interés por el sistema, que son señalados con (*).
- El usuario selecciona la opción de enviar.
- Los datos ingresados en los campos de interés, son verificados por el sistema.
- Se guarda la información relacionada con login y password en la tabla usuario, los datos relacionados con su perfil son almacenados en el registro usuario de la base de datos.
- Se cierra la pantalla de registro de usuario.
- Se emite una pantalla con la página inicio, donde el usuario puede acceder al sistema como administrador.

2.2 FLUJO DE EVENTOS

Se emite una pantalla de error por campo de interés sin llenar o que los datos estén mal ingresados (numero de caracteres de login y password), a su ves los usuarios que ya existen no pueden crearse de nuevo.

3. REQUERIMIENTOS ESPECIALES

La persona que ingrese al registro de usuario, será porque no se encuentra registrada en el sistema.

4. POSCONDICIONES

Su registro al sistema ha sido satisfactorio.

5. PUNTOS DE EXTENSIÓN

El usuario, después de haber sido registrado e el sistema podrá acceder a las opciones recopilación de Información o preparación de auditorias. Si se accede a alguna de estas dos opciones, se puede acceder a los cuestionarios. Además de esto tiene las opciones que tiene un usuario normal como son: ver glosario, Ver información general y Salir.

ACTOR: USUARIO – ADMINISTRADOR

EVENTO: VER GLOSARIO

1. DESCRIPCIÓN

Se solicita la visualización del glosario almacenado en el sistema de la base de datos. El usuario, ya sea con o sin privilegios puede acceder a esta opción con el fin de entender mejor el SGSI (Sistema de gestión de seguridad de Información) y la norma ISO 17799.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- El usuario accede a la página principal
- Se muestra una ventana con la opción seleccionada “Ver glosario”
- El usuario selecciona la letra que desea ver
- El usuario busca la palabra a consultar y da clic
- El sistema muestra la información de la palabra seleccionada

2.2 FLUJO ALTERNATIVO

El usuario sale del sistema sin realizar cambios

3. PRECONDICIONES

Las bases de datos se encuentran habilitadas por el administrador de la Web.

4. POSCONDICIONES

El usuario visualiza el glosario que requería y puede acceder a otro enlace

ACTOR USUARIO – ADMINISTRADOR

EVENTO: VER INFORMACIÓN GENERAL SGSI

1. DESCRIPCIÓN

Describe el proceso de solicitud de visualización de información general almacenando en el sistema de la base de datos. El usuario ya sea con o sin privilegios puede acceder a esta opción con el fin de entender mejor el SGSI (Sistema de Gestión de Seguridad de Información) y la norma ISO 17799.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- El usuario accede a la pagina principal
- Se muestra una ventana de la opción seleccionada “Información General”
- El usuario tiene la opción de ver la información en la página o acceder a artículos de documentación de la ISO 17799.

2.2 FLUJO ALTERNATIVO

El usuario sale del sistema sin realizar cambios

3. PRECONDICIONES

Las bases de datos de información se encuentran habilitadas por el administrador de la Web.

4. POSCONDICIONES

El usuario visualizo información general que requería y puede acceder a otro evento.

ACTOR: ADMINISTRADOR

EVENTO: VERIFICAR IDENTIDAD

1. DESCRIPCIÓN

Este proceso representa la validación del autenticidad del administrador para acceder al sistema, para esto necesita digitar un login y un password.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- El administrador ingresa a la ventana de identificación
- Digita login y password correspondientes a el asignado a el usuario ya registrado.
- El login y password ingresados son validados por el sistema, verificando en la base de datos que los datos se encuentren en el sistema y que sean correctos.
- Se autoriza el ingreso al menú principal.

2.2 FLUJO ALTERNATIVO

- Si alguno de los datos ingresados no son validos, el sistema devuelve la misma interfaz en espera de que se ingresen datos validos
- El administrador sale del sistema sin realizar cambios

3. REQUERIMIENTOS ESPECIALES

Login y password del administrador se encuentran almacenados en la tabla de usuario.

4. POSCONDICIONES

Su ingreso al sistema ha sido satisfactorio

5. PUNTOS DE EXTENSIÓN

El administrador por ser usuario del sistema pero con beneficios de administrador podrá tener acceso a las mismas opciones de menú ofrecidas a un usuario normal, pero también tendrá las opciones adicionales de registro, recopilación de información y preparación de auditorias.

ACTOR: ADMINISTRADOR

EVENTO: PREPARACIÓN DE AUDITORIAS

1. DESCRIPCIÓN

Describe el proceso de evaluar cuestionarios sobre la seguridad de información en las organizaciones, este evento muestra los diferentes cuestionarios que existen de acuerdo a controles tomados de la norma técnica ISO 17799. En este caso el usuario podrá calificar de acuerdo a el ítem que desee (ejemplo: políticas de seguridad).

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

El usuario después de acceder al sistema como administrador con un login y un password, accede al menú principal del prototipo, selecciona preparación de auditorias y se le muestra una serie de ítems u opciones que el usuario escoge de acuerdo a sus preferencias, lo evalúa y por último el sistema se encarga de mostrarle una respuesta en la cual le da un porcentaje de seguridad con la que se cuenta en la empresa de acuerdo a lo que se respondió.

2.2 FLUJO ALTERNATIVO

El usuario sale del sistema sin realizar cambios, simplemente se encarga de responder cuestionarios y decidir si desea o no ver el registro de cuestionarios con respuesta y sus respuestas.

3. REQUERIMIENTOS ESPECIALES

El usuario esta asignado al registro de usuarios o registrado en el sistema, se debe responder con anterioridad los cuestionarios del ítem Recopilación de Información con el fin de accede a el evento Preparación de Auditorias.

4. PRECONDICIONES

El usuario esta registrado en el sistema

Existen cuestionarios en la base de datos local, para ser calificados y evaluados.

ACTOR: ADMINISTRADOR

EVENTO: SOLICITAR PAGINA

1. DESCRIPCIÓN

Este es el proceso, en donde el usuario hace una solicitud de visualizar la pagina donde se encuentra el prototipo desarrollado, accediendo a la pagina principal del administrador con un login y un password.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

- Se accede a la ventana principal como usuario normal
- El usuario selecciona la opción Inicio
- Se despliega un formulario donde aparece la solicitud de login y password para acceder al sistema como usuario administrador.
- Se realiza un verificación de login y password
- La Web muestra las opciones que existen para el administrador.

2.2 FLUJO ALTERNATIVO

El usuario sale del sistema sin realizar cambios, simplemente responde los cuestionarios que desea responder.

3. PRECONDICIONES

El usuario debe estar registrado en el sistema

4. POSCONDICIONES

El sistema muestra dos opciones de cuestionarios para evaluar.

5. PUNTOS DE EXTENSIÓN

- Recopilación de Información
- Preparación de auditorias

ACTOR: ADMINISTRADOR

EVENTO: RECOPILAR INFORMACIÓN

1. DESCRIPCIÓN

Describe le proceso de evaluar cuestionarios de seguridad de información de organizaciones, este evento muestra una bienvenida y un botón de acceso a cuestionarios. El usuario solo puede dar calificaciones a los ítems pertenecientes a la base de datos.

2. FLUJO DE EVENTOS

2.1 FLUJO BÁSICO

El usuario después de acceder al sistema como administrador con un login y un password, accede a un menú principal, donde selecciona Recopilar Información y de allí se despliega una serie de cuestionarios donde el usuario evalúa y después se muestran los resultados con el fin de realizar luego la auditoria.

2.2 FLUJO ALTERNATIVO

Se espera a verificar si el usuario quiere continuar evaluando o si simplemente desea salir del sistema.

3. REQUERIMIENTOS ESPECIALES

El usuario debe estar asignado al registro usuario.

4. PRECONDICIONES

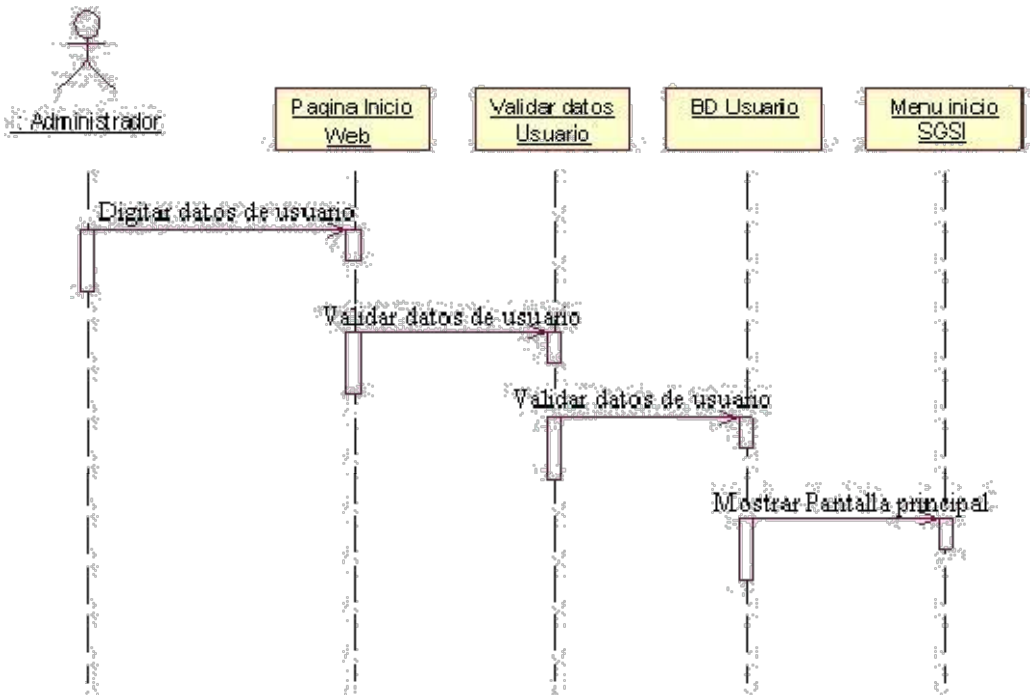
El usuario debe estar registrado en el sistema

5. POSCONDICIONES

Se puede acceder al ítem preparación de auditorias para evaluar los cuestionarios de este.

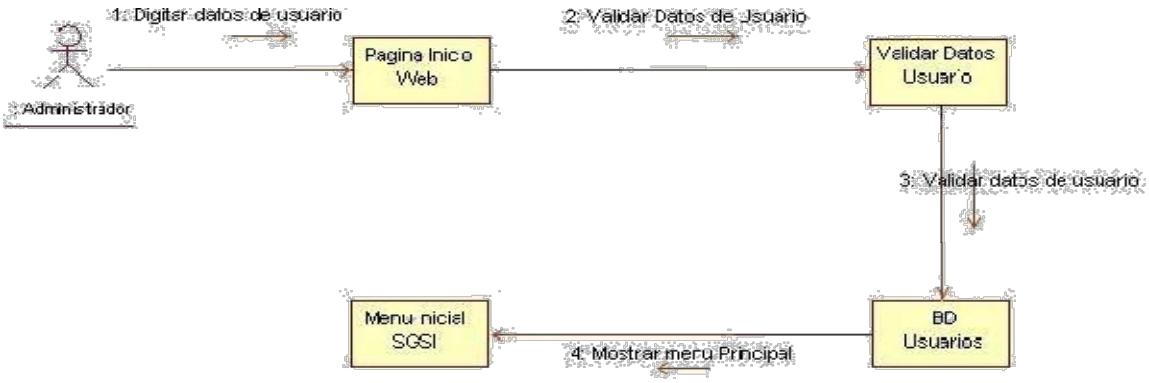
Anexo C. Diagrama de secuencia y colaboración

Figura 24. Diagrama De Secuencia "Verificar Identidad"



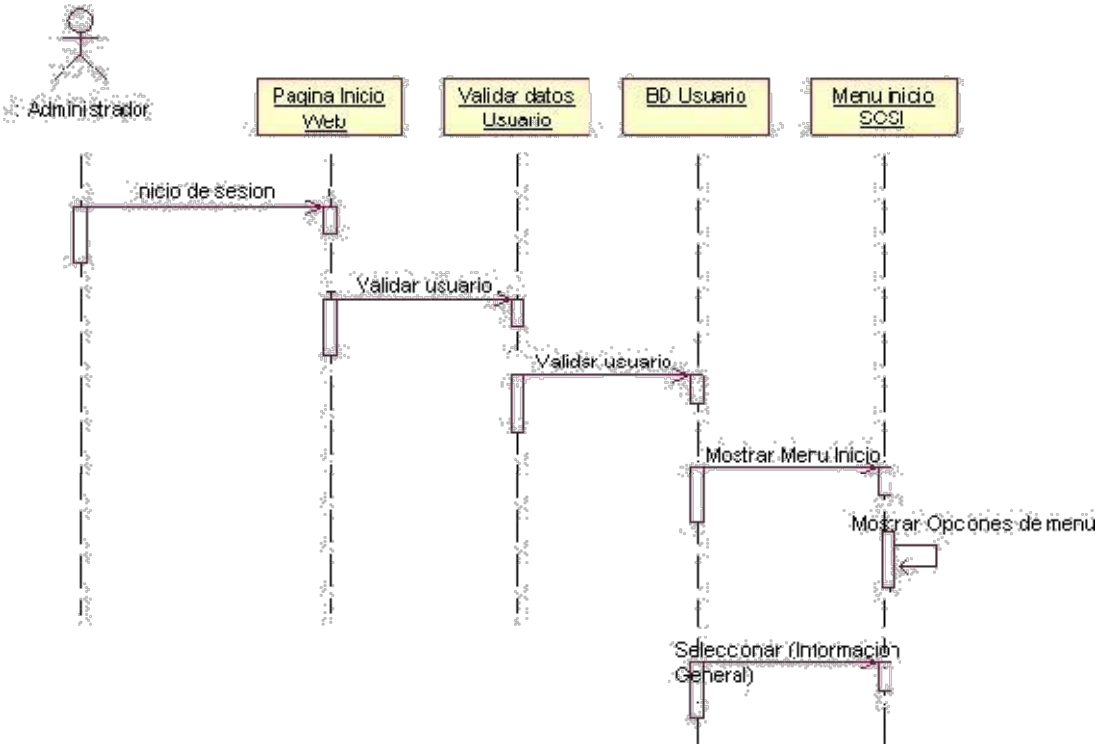
Fuente: Autores del Proyecto

Figura 25. Diagrama de Colaboración "Verificar Identidad"



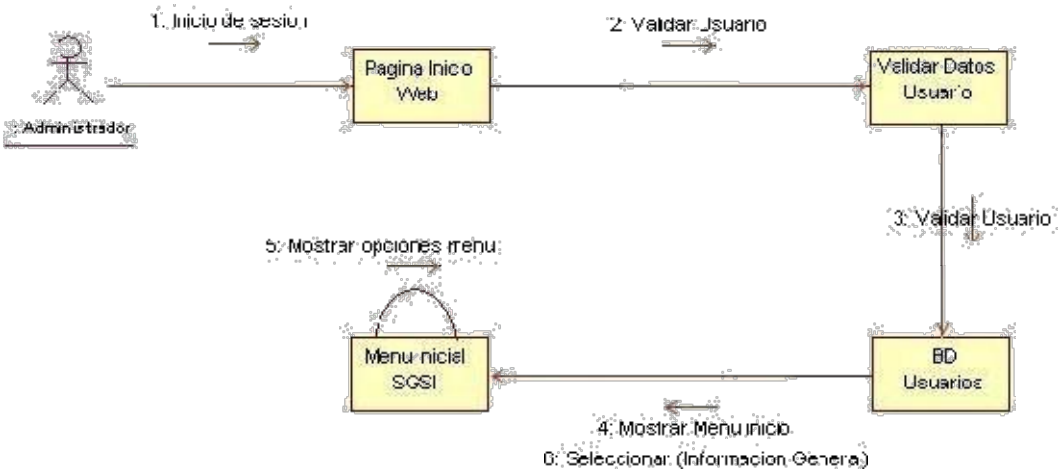
Fuente: Autores del Proyecto

Figura 26. Diagrama de Secuencia "Ver Información ISO 17799"



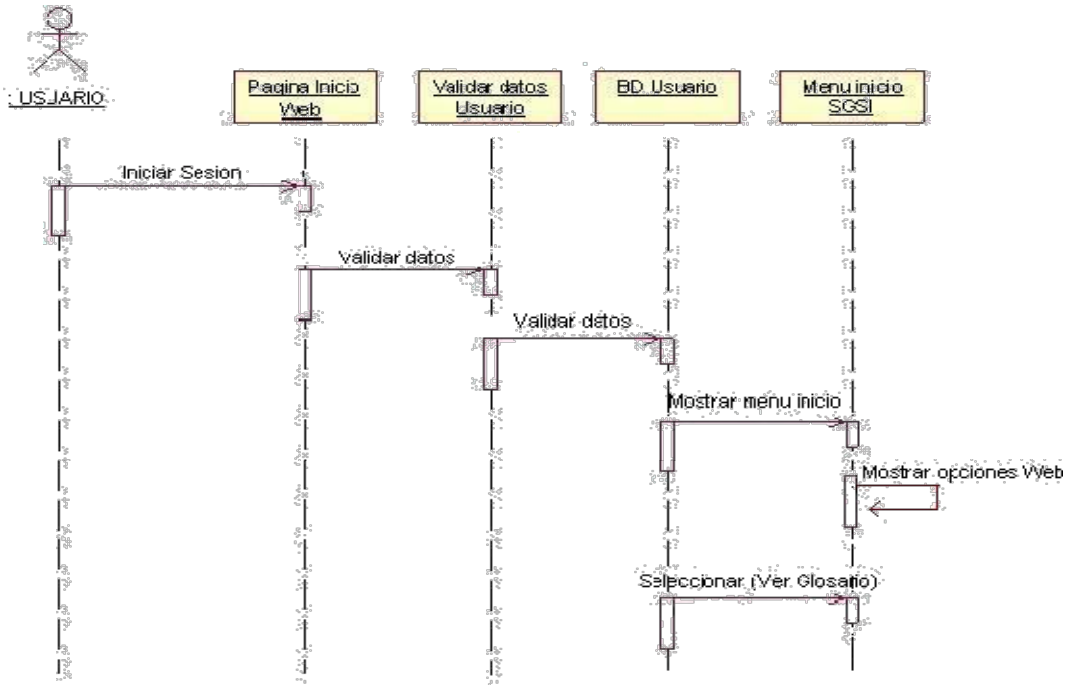
Fuente: Autores del Proyecto

Figura 27. Diagrama de Colaboración "Ver Información ISO 17799"



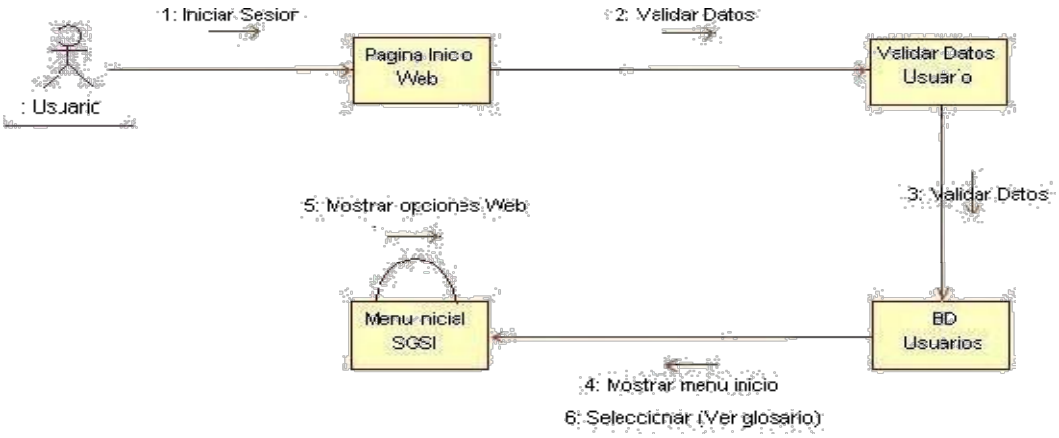
Fuente: Autores del Proyecto

Figura 28. Diagrama de Secuencia "Ver Glosario"



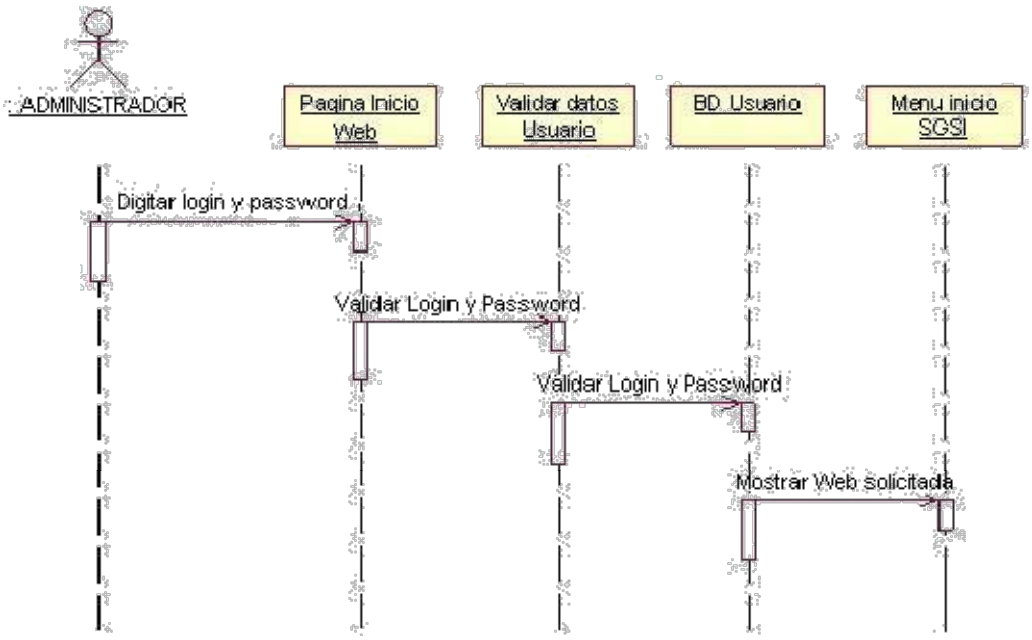
Fuente: Autores del Proyecto

Figura 29. Diagrama de Colaboración "Ver Glosario"



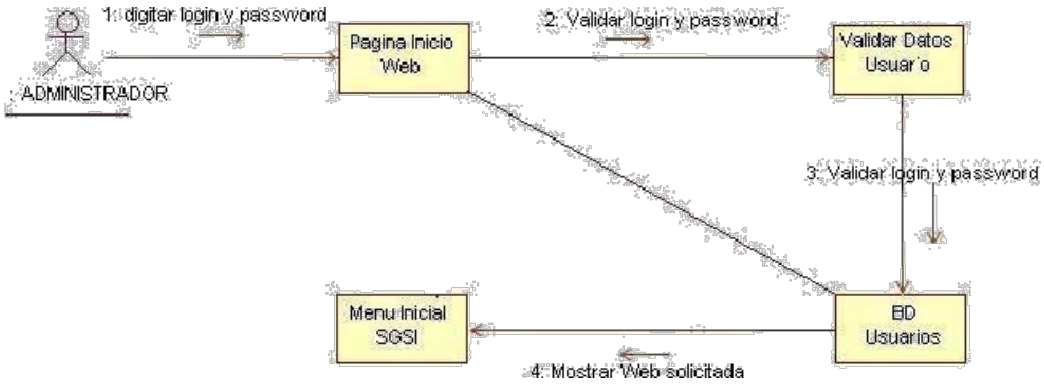
Fuente: Autores del Proyecto

Figura 30. Diagrama de Secuencia "Solicitar Pagina"



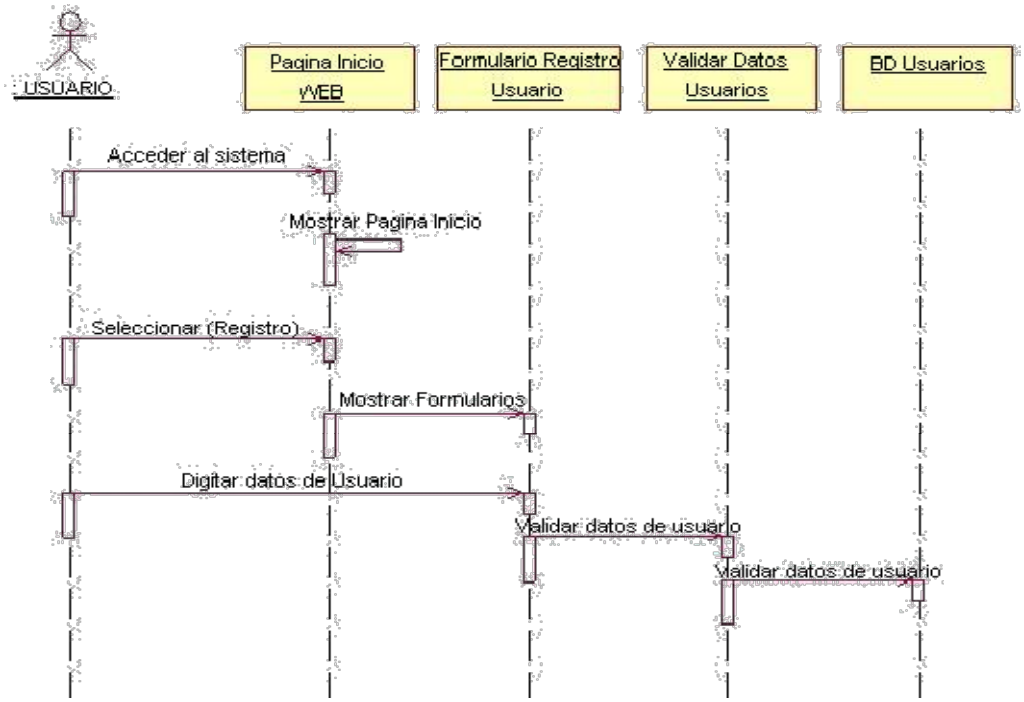
Fuente: Autores del Proyecto

Figura 31. Diagrama de Colaboración "Solicitar Pagina"



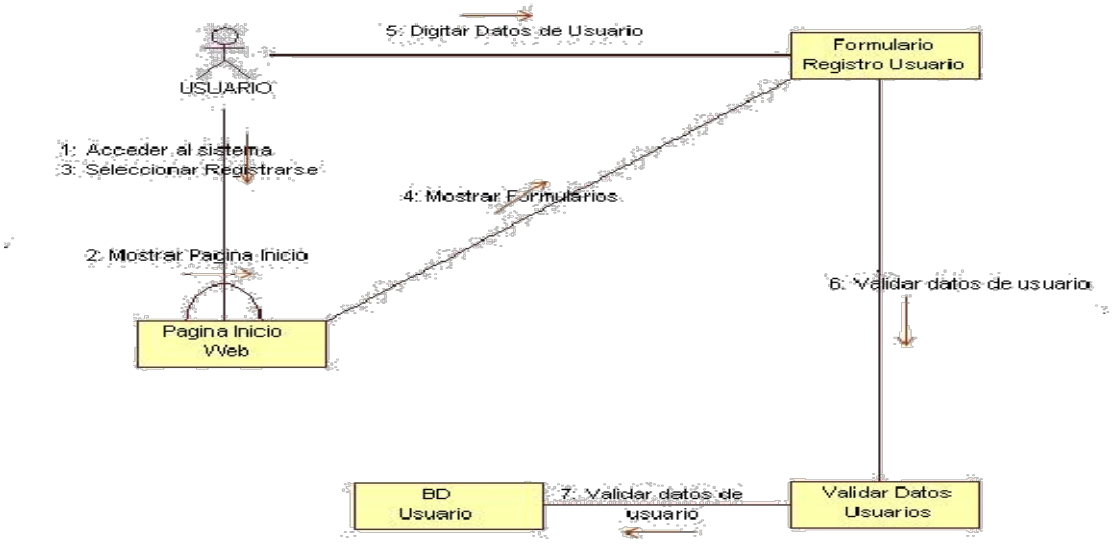
Fuente: Autores del Proyecto

Figura 32. Diagrama de Secuencia "Registrarse en el sistema"



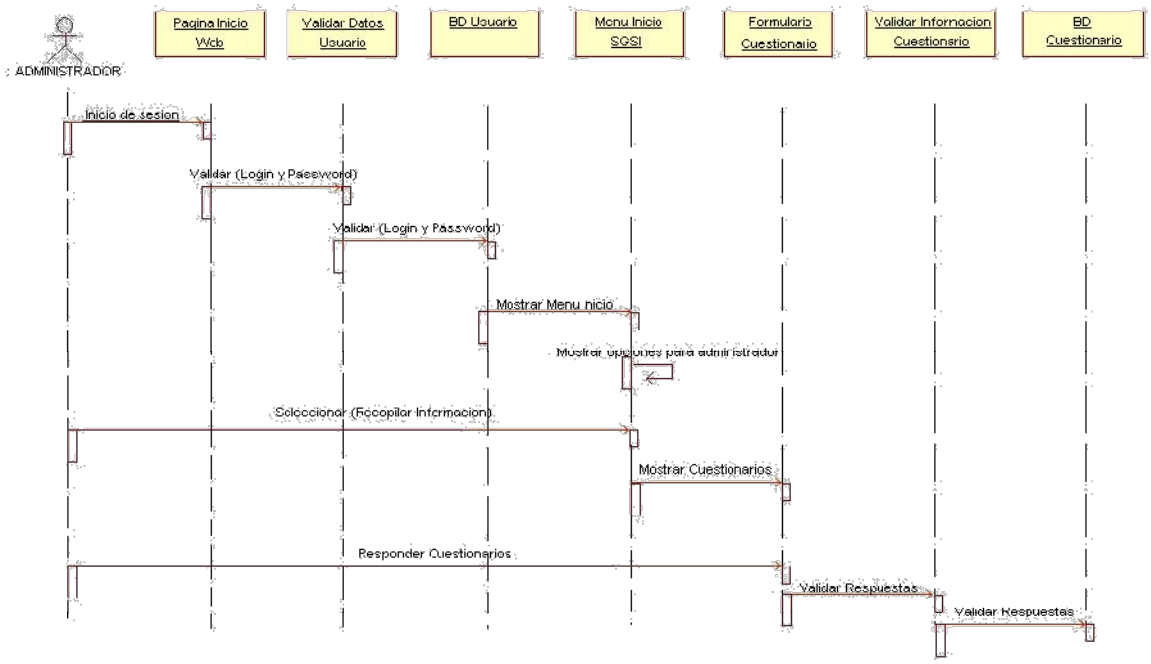
Fuente: Autores del Proyecto

Figura 33. Diagrama de Colaboración "Registrarse en el sistema"



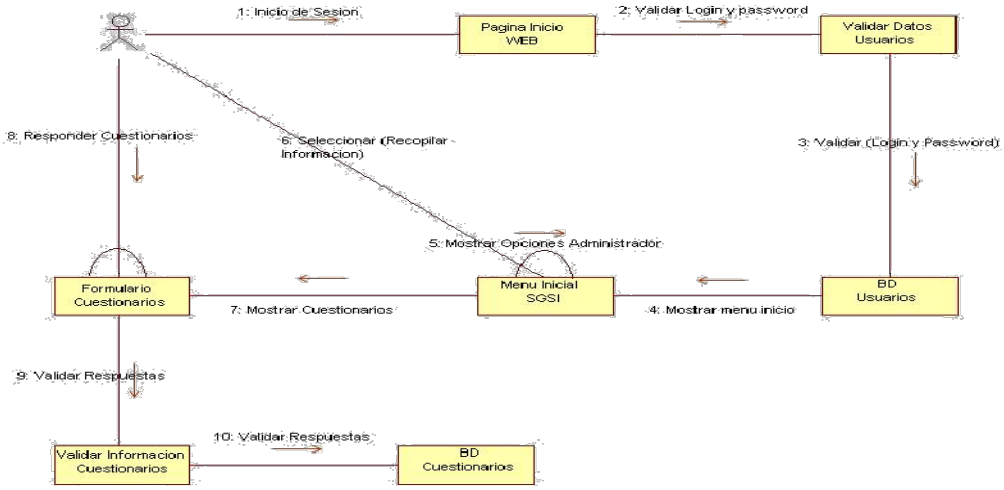
Fuente: Autores del Proyecto

Figura 34. Diagrama de Secuencia "Recopilar Información"



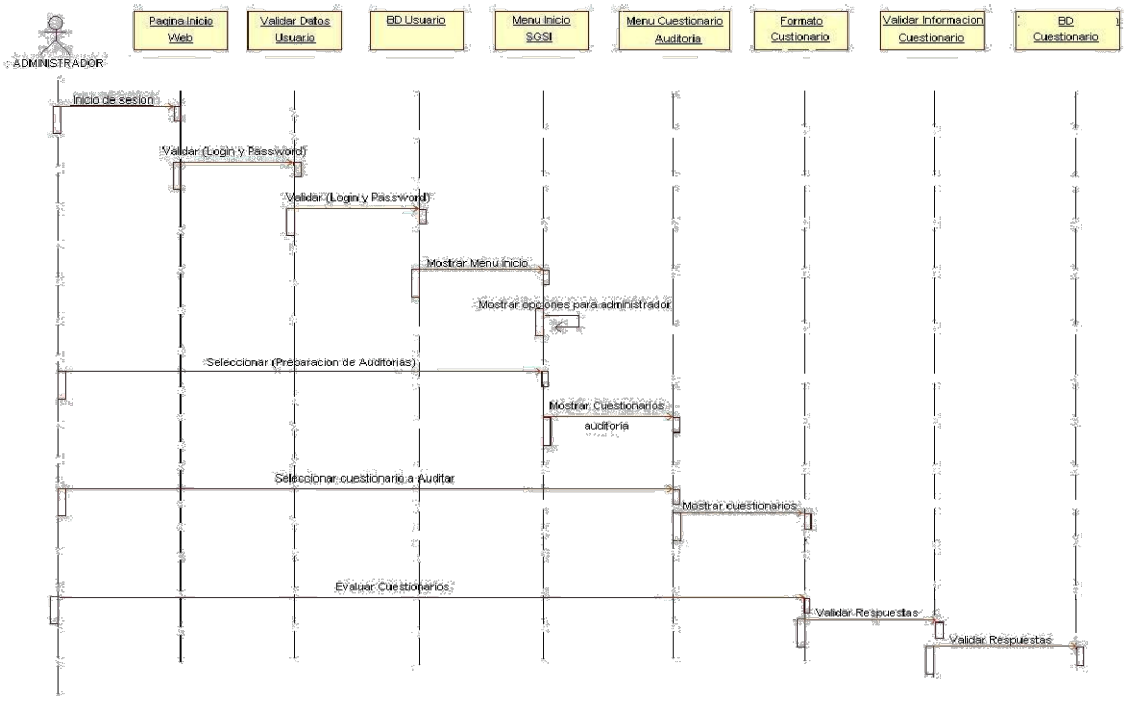
Fuente: Autores del Proyecto

Figura 35. Diagrama de Colaboración “Recopilar Información”



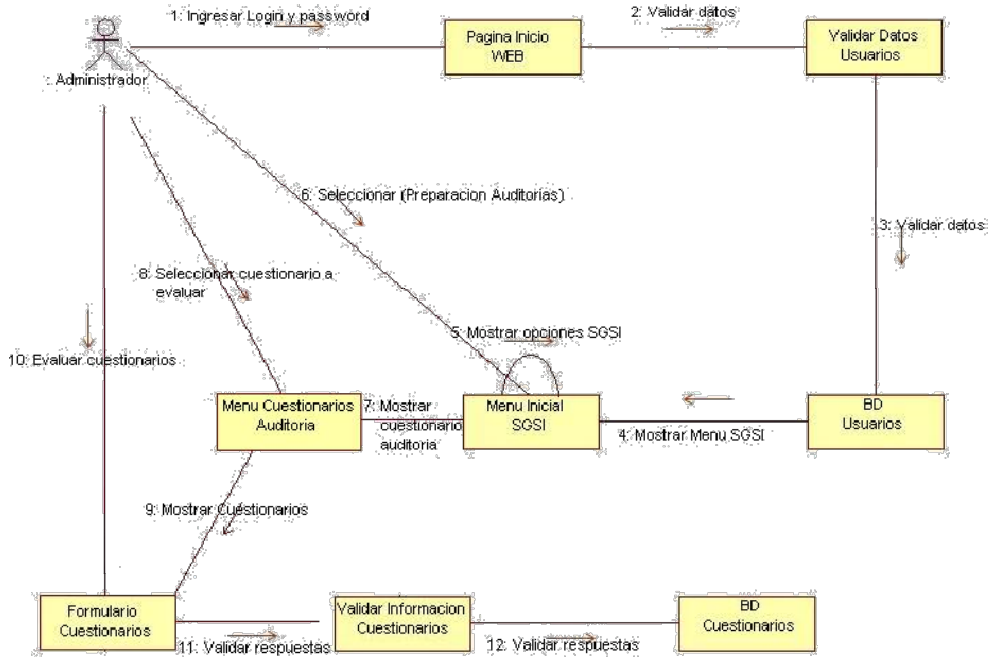
Fuente: Autores de Proyecto

Figura 36. Diagrama de Secuencia “Preparación de Auditorias”



Fuente: Autores de Proyecto

Figura 37. Diagrama De Colaboración "Preparación De Auditorias"



Fuente: Autores de Proyecto