UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

Sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y GESTION DEL RIESGOS INFORMÁTICOS

ASESOR:
MG. JOSÉ REMBERTO GUTIERREZ ALVARADO

PRESENTADO POR:

LEONARDO JOSÉ CASTILLO PERLA

HENRRY BLADIMIR FLORES RIVERA

OSCAR AGUSTÍN RODRÍGUEZ UMAÑA

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Enero de 2015

AGRADECIMIENTOS:

Quiero Agradecer A Dios y la Virgen María por la vida y sus bendiciones en todos los pasos necesarios que han llevado a culminar una meta como es la Maestría.

A mi esposa Marta y mi hija Sonia que me acompañaron en este reto con mucho amor les agradezco por ser la inspiración para superarme constantemente y me quedo sin palabras para agradecer su apoyo y comprensión el cual ha sido incondicional.

A mis Padres por toda su ayuda, guía y ejemplo por lo cual es ahora posible este logro académico y personal, de igual forma agradezco a mi demás familia que de alguna u otra forma fueron un apoyo constante en estos dos años.

Compartir esta alegría con mis amigos y demás compañeros de Avianca por ser un sustento y fuente de consejos y ánimos, sin ellos no hubiese sido posible culminar mis estudios.

Finalmente a mis compañeros de equipo Henrry, Oscar, Ricardo, Roberto y demás compañeros de la Maestría les agradezco su amistad y por todo lo aprendido, finalmente se culmina esta aventura.

Leonardo José. Castillo Perla

AGRADECIMIENTOS:

Quiero agradecer a Dios por la vida y sus bendiciones en todos los pasos necesarios que han llevado a culminar una meta como es la Maestría en Seguridad Informática.

A mi esposa Kriscia que me acompañaron en este reto, con mucho amor, les agradezco por ser la inspiración para superarme constantemente, agradezco su apoyo y comprensión el cual ha sido incondicional.

A mis padres José Lorenzo Flores y Maria Rosario de Flores por toda su apoyo, guía y ejemplo por lo cual es ahora posible este logro académico y personal.

A la Universidad Don Bosco y mis compañeros de trabajo por brindarme su conocimiento y apoyo en la maestría.

Finalmente a mis compañeros de estudio Leonardo, Oscar, Roberto, Ricardo y demás compañeros de la Maestría, les agradezco su amistad, compañerismo y por todo lo aprendido, finalmente se culmina esta aventura.

Henrry Bladimir Flores Rivera

AGRADECIMIENTOS:

En primer lugar, quiero agradecer a Dios todopoderoso por haberme ayudado a enfrentar y salir adelante de este reto.

Quiero agradecer a mi madre Sonia María, que sé que desde el cielo ha estado guiando mis pasos para mi desarrollo profesional y personal.

A mi padre, por su apoyo incondicional, consejos y ejemplo a seguir.

Al equipo docente y personal administrativo de la maestría, por la transmisión de sus conocimientos y las capacitaciones brindadas durante el largo de la maestría.

A mis compañeros de grupo, con quienes nos hemos esforzado y desvelado para lograr el fin que nos hemos propuesto.

A mis colegas y amigos que me han aconsejado y guiado para el desarrollo de mis estudios.

Oscar Agustín Rodríguez Umaña

Sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco

Castillo Perla, Leonardo J.; Flores Rivera, Henrry B.; Rodríguez Umaña, Oscar A.
leonardojcastillop@gmail.com. bladimirfloresr@gmail.com. oscar.rodriguez202@gmail.com
Universidad Don Bosco, El Salvador

***Resumen*—En los últimos años, el tema de seguridad de la información ha ido en aumento, con los avances en las tecnologías de la información que permiten cada vez mejores herramientas de comunicación entre individuos y organizaciones, así mismo han aumentado las herramientas y metodologías que tratan de vulnerar, modificar o robar información, consideradas por las organizaciones como uno de sus activos más importantes. Tal es el caso que Organización de Estándares Internacionales (OSI por sus siglas en inglés) han desarrollado marcos de referencia y estándares que permiten a las organizaciones proteger su información al minimizar en la medida de lo posible y mediante revisiones periódicas de estos estándares, las vulnerabilidades y riesgos resultantes de las mismas sobre sus activos. El Sistema SGSI permite a las organizaciones la implementación y mantenimiento de un Sistema de la Seguridad de la Información, conforme a los estándares establecidos en la norma ISO 27001. El presente artículo trata sobre las funcionalidades de dicho sistema y las directrices sobre las que está desarrollado.**

***Índice de términos*—Sistema de Gestión de la Seguridad Informática, Seguridad Informática, SGSI, Software.**

I. Introducción

Un Sistema de Gestión de la Seguridad Informática (SGSI) es un proceso definido que sirve para evaluar, implementar, mantener y administrar la seguridad de la información de una organización y que apoya a la misma el logro de sus metas, que además dentro del contexto de la Universidad Don Bosco apoya de igual forma en la consecución de la visión que tiene la Universidad en la gestión del conocimiento y mejoramiento continuo de calidad que son partes que las normas ISO que son exigidas y a la vez apoyan.

La Universidad Don Bosco es un referente en la enseñanza de la ciencia y tecnología en el país y el poseer un marco de referencia como es la ISO27001 permite ser un ejemplo a seguir con una buena práctica y ser un modelo a las distintas audiencias que están pendientes de los pasos y guías que dicta la Universidad Don Bosco y permite ser un diferenciador más con respecto a la competencia.

Para una organización, contar con un sistema para la implementación, mantenimiento y monitoreo de un SGSI es un indicador de la madurez y el compromiso de la misma para garantizar que exista una seguridad razonable a lo largo de toda la organización, y a su vez también genera valor para las partes interesadas, generando una mejor percepción que se tiene de la opinión pública para la organización.

El siguiente documento describe las consideraciones que se deben tomar en cuenta en el establecimiento de un sistema de Gestión de Seguridad de Información (SGSI) junto con los requerimientos que son exigibles por la norma, así como los controles sugeridos por la mejor práctica.

II. OBJETIVO GENERAL

Desarrollar un sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco el cual cumpla con todos los requerimientos de la norma ISO27001:2005 y que sea una guía para su cumplimiento y certificación.

II. OBJETIVOS ESPECÍFICOS

- Establecer una metodología de análisis, evaluación y tratamiento de riesgo, el cual sea gestionado por el sistema propuesto y que cumpla con el estándar de la norma IS027001:2005.
- Identificar y administrar los controles sugeridos por la ISO27002 de mejores prácticas, los cuales puedan ser actualizados constantemente y se les pueda asignar un dueño, conforme a las necesidades de la Universidad Don Bosco
- Contar con un sistema que permita a la Universidad Don Bosco identificar los requerimientos necesarios para la certificación de la ISO27001:2005

III. JUSTIFICACIÓN

La Universidad Don Bosco en su actualidad no posee un sistema de gestión de seguridad de información y al ser un referente Tecnológico en el país es de suma importancia que cuente con un marco de referencia para la gestión de la

seguridad de la información y de igual forma generar valor a las partes interesadas de la Universidad, en base a lo observado se posee elementos aislados que pudieran ser parte de ese sistema para el alcance dentro de la organización sea conforme a lo definido por la norma.

IV. ALCANCES

Contar con un sistema de información que le permita a la Universidad Don Bosco visualizar los requerimientos que son necesarios para cumplir con la norma ISO27001:2005 y a su vez poder gestionar los controles definidos como buenas prácticas conforme a la ISO27002 Controles de seguridad de información, el cual podrá ser utilizado desde ambientes (Aplicaciones Windows y Web), y dispositivos (Computadoras y dispositivos móviles)

La arquitectura del sistema estará constituida por diversas capas que está conformada desde la comunicación de la base de datos y la Interfaces gráficas con los usuarios finales, esta arquitectura será mediante el desarrollo de una librería específica entre las Interfaces y la base de datos, permitiendo así la modularidad del sistema, para permitir la comunicación entre diferentes dispositivos y ambientes.

V. LIMITANTES

Para Implementar el SGSI en la Universidad Don Bosco es necesario que se efectué mediante un proyecto en el cual se incluya a representantes de las principales áreas de la organización, para asegurarse que se contemplen todas las áreas y procesos que necesitan estar bajo la sombrilla del sistema de Gestión, con el alcance adecuado conforme a las necesidades de la Universidad. A su vez que se designen responsabilidades y recursos para garantizar que el desarrollo del proyecto cumpla con los objetivos definidos por la norma y la certificación del SGSI para la UDB.

Este apoyo y compromiso por parte de la Universidad es necesario para el desarrollo de este proyecto de graduación, el cual es de vital importancia para poder implementar el sistema para que este proyecto de graduación sea una guía y un recurso que permita gestionar los requerimientos de la norma ISO27001 y a su vez delimitar las necesidades de las diferentes áreas definidas dentro del alcance y que estas generen valor para la organización.

VI. MARCO TEÓRICO

La Universidad Don Bosco es una institución educativa de nivel superior, de utilidad pública, apolítica, de inspiración cristiana y sin fines de lucro.

La responsabilidad de la Universidad Don Bosco ante los desafíos de la sociedad ha propiciado el establecimiento de iniciativas institucionales significativas, tales como la construcción del Modelo Educativo, la planificación estratégica y táctica de largo y mediano plazo y la construcción de una institucionalidad e integridad cada vez más orientada a la mejora continua[1].

La Universidad Don Bosco es un referente al ofrecer una oferta académica que es innovadora en estudios de pregrado, maestrías, postgrados, cursos especializados en temas de ciencias y tecnología, por lo cual es una necesidad imperiosa contar con una estructura y ambiente de control basado en una norma como es la ISO27001 y que a su vez también es una buena práctica y que sea mediante la gestión de un SGSI de igual forma se predique con el ejemplo y se consolide aún más como un referente con los estudios que son promulgados desde las aulas de la Universidad.

La seguridad de la información es un aspecto y un concepto que tiene que ser contemplando por la Universidad Don Bosco y por toda organización, las cuales están compuestas por información que es un activo, que, como otros activos comerciales importantes, es esencial para el negocio y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La información puede existir en muchas formas, independientemente de la forma o medio por el cual sea almacenado o compartido, siempre debería estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementado un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan con los objetivos de seguridad y comerciales específicos [1].

Mediante un marco de control como la ISO27001 SGSI (Sistema de Gestión de Seguridad de la Información) estos ayudan a asegurar que se cumplan los requisitos de seguridad y privacidad, muchas organizaciones adoptan marcos de control para proporcionar un programa de gobierno, que es:

1. Consistente: Un programa de gobierno debe ser coherente en, cómo se aborda y se aplican seguridad de la

información y la privacidad. Si dos situaciones o solicitudes similares producen resultados diferentes, los actores van a perder la fe en la integridad del programa y su utilidad.

2. Medibles: El programa de gobierno debe proporcionar una forma de determinar el progreso y establecer metas. Las organizaciones que implementan los marcos que se pueden medir son más propensos a mejorar su situación de seguridad en el tiempo. La mayoría de los marcos de control contienen una norma o procedimiento de evaluación para determinar el cumplimiento y en algunos casos el riesgo también.

3. Estandarizado: Al igual que con medible anteriormente, un marco de controles debe basarse en la normalización para que los resultados de una organización o parte de una organización se pueden comparar de una manera significativa.

4. Integral: El marco seleccionado debe cubrir los requisitos legales y reglamentarios mínimos de una organización y ser extensible para dar cabida a los requisitos específicos de organización adicional.

5. Modular: un marco modular es más probable, que soportar los cambios de una organización, ya que sólo los controles o requisitos que se desee modificar son revisados y actualizados[2].

La ISO27001 establece los requerimientos formales para la implementación de un Sistema de Gestión de Seguridad de la Información y forma parte de la familia de la ISO27000 [5] que componen más de 30 normas específicas y que a su vez establecen los términos y definiciones que son aplicables a todos los demás componentes de la norma.

Para el Sistema de Gestión de Seguridad de la Información el único estándar certificable es la ISO27001, el cual específica formalmente todos los requerimientos exigidos por la norma y el cual es una serie de actividades referentes a la administración de los riesgos de seguridad que consiste en la identificación, análisis y tratamiento de los riesgos informáticos, el SGSI asegura que los arreglos de seguridad se encuentren alineados para estar conforme a los cambios de las amenazas de seguridad, vulnerabilidades e impacto al negocio que suele ser tan cambiante. La norma no impone controles específicos de seguridad de la información [3].

ISO27002:2005

Para el desarrollo del Sistema de Gestión de Seguridad de la Información se utilizó la ISO / IEC 27002 como referencia de los controles utilizados dado que es un estándar internacionalmente reconocido de buenas prácticas para la seguridad de la información y se remonta su historia de más de 30 años para sus precursores de la BS 7799.

Este estándar se refiere explícitamente a la seguridad de la información, es decir, la seguridad de todas las formas de información (por ejemplo, datos informáticos, la documentación, el conocimiento y la propiedad intelectual) y no sólo de TI.

El uso de la ISO/IEC 27002 es como una mejor práctica o una guía para indicar los controles de seguridad adecuados o sugeridos dentro de un SGSI los cuales son 11 dominios con 39 objetivos de control y 133, pero estos no son un estándar de certificación, ya que para la familia de la ISO27000 la única certificable como se mencionó anteriormente es la norma ISO27001 [4].

Historia

ISO / IEC 27001 se deriva de la norma Británica BS 7799 Parte 2, publicado en 1999. BS 7799 Parte 2, fue revisada por BSI en 2002, la incorporación del ciclo de Deming: Planificar – Hacer –Verificar – Actuar, concepto proceso cíclico, y fue adoptado por la norma ISO / IEC como ISO / IEC 27001 en 2005. Fue revisado extensamente en 2013, alineándola con las otras normas de sistemas de gestión ISO certificada y adoptando el concepto PDCA.

Requerimientos Mandatorios para la Certificación

a. Alcance del SGSI (según la cláusula 4.3)

b. La política de seguridad de la información (cláusula 5.2)

c. Proceso de evaluación de riesgos de seguridad de la información (cláusula 6.1.2)

d. Proceso de tratamiento de riesgos de seguridad de la información (cláusula 6.1.3)

e. Los objetivos de seguridad de la información (cláusula 6.2)

f. Evidencia de la competencia de las personas que trabajan en seguridad de la información (cláusula 7.2)

g. Otros documentos relacionados con el SGSI considerados necesarios por la organización (7.5.1b cláusula)

h. Documentos de planificación y control operacional (cláusula 8.1)

i. Los resultados de las evaluaciones de riesgos (cláusula 8.2)

j. Las decisiones con respecto al tratamiento del riesgo (cláusula 8.3)

k. La evidencia de la supervisión y medición de la seguridad de la información (cláusula 9.1)

l. El programa de auditorías internas SGSI y los resultados de las auditorías realizadas (cláusula 9.2)

m. Evidencia de las principales revisiones de la gestión de los SGSI (cláusula 9.3)

n. La evidencia de las no conformidades identificadas y acciones correctivas derivadas (cláusula 10.1)

o. Otros varios: Anexo A
   - Reglas para el uso aceptable de los activos
   - Política de control de acceso
   - Procedimientos operativos
   - Acuerdos de confidencialidad o de no divulgación.
   - Política de seguridad de la información para relaciones con los proveedores. [6]

VII. TECNOLOGÍAS

Para el desarrollo del Sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco la tecnología identificada es la siguiente.

A. Microsoft .NET Framework 4

NET Framework es el modelo de programación completo y coherente de Microsoft para compilar aplicaciones que ofrezcan una sensacional experiencia visual del usuario, comunicación perfecta y segura, y la capacidad de modelar una amplia gama de procesos empresariales.NET Framework 4 funciona en paralelo con versiones anteriores de .NET Framework. Las aplicaciones basadas en versiones anteriores de .NET Framework continuarán ejecutándose en la versión que tienen definida como destino de forma predeterminada. Microsoft .NET Framework 4 proporciona las siguientes mejoras y características nuevas*:*

- Mejoras en Common Language Runtime (CLR) y la biblioteca de clases base (BCL)
- Innovaciones en los lenguajes Visual Basic y C#; por ejemplo, lambdas de instrucciones, continuaciones de línea implícitas, distribución dinámica y parámetros con nombre u opcionales.
- Mejoras en el acceso a datos y el modelado
- Mejoras en ASP.NET
- Mejoras en Windows Presentation Foundation (WPF)
- Mejoras en Windows Workflow (WF) que permiten a los desarrolladores hospedar mejor e interactuar con flujos de trabajo. Estas mejoras incluyen un modelo de programación de actividades mejorado, un mejor funcionamiento del diseñador, un nuevo estilo de modelado de diagramas de flujo, una paleta de actividades expandida, integración con reglas de flujos de trabajo y nuevas características de correlación de mensajes. .NET Framework 4 ofrece también una mejora notable en el rendimiento para flujos de trabajo basados en WF.
- Mejoras en Windows Communication Foundation (WCF), como la compatibilidad con Servicios de flujos de trabajo de WCF, que permiten programas con actividades de mensajería y correlación. Además, .NET Framework 4 proporciona nuevas características de WCF como la detección de servicios, servicio de enrutamiento, compatibilidad con RES, diagnósticos y rendimiento.
- Nuevas características de programación en paralelo, como la compatibilidad con bucles en paralelo, biblioteca en paralelo de tareas (TPL), LINQ paralelo (PLINQ) y estructuras de datos de coordinación que permiten a los desarrolladores aprovechar la eficacia de procesadores multinúcleo. [7]

B. ASP.NET y Visual Studio para Web

ASP.NET es una plataforma web que proporciona todos los servicios necesarios para compilar aplicaciones web empresariales basadas en servidor. ASP.NET está compilado en .NET Framework, por lo que todas las características de .NET Framework están disponibles en las aplicaciones ASP.NET. Las aplicaciones se pueden escribir en cualquier lenguaje que sea compatible con Common Language Runtime (CLR), incluido Visual Basic y C#.

ASP.NET es un modelo de desarrollo Web unificado que incluye los servicios necesarios para crear aplicaciones Web empresariales con el código mínimo. ASP.NET forma parte de .NET Framework y al codificar las aplicaciones ASP.NET tiene acceso a las clases en .NET Framework. El código de las aplicaciones puede escribirse en cualquier lenguaje compatible con el Common Language Runtime (CLR), entre ellos Microsoft Visual Basic, C#, JScript .NET y J#. Estos lenguajes permiten desarrollar aplicaciones ASP.NET que se benefician del Common Language Runtime, seguridad de tipos, herencia, etc. [9]

ASP.NET incluye:

- Marco de trabajo de página y controles
- Compilador de ASP.NET

- Infraestructura de seguridad
- Funciones de administración de estado
- Configuración de la aplicación
- Supervisión de estado y características de rendimiento
- Capacidad de depuración
- Marco de trabajo de servicios Web XML
- Entorno de host extensible y administración del ciclo de vida de las aplicaciones
- Entorno de diseñador extensible

C. SQL Server 2008 R2

Microsoft SQL Server 2008 R2 Express con Service Pack 2 es una edición gratuita y con muchas características de SQL Server que resulta idónea para aprender, desarrollar y activar pequeñas aplicaciones de servidor, web y de escritorio, así como para su redistribución a través de ISV. [8]

D. Windows Communication Foundation (WCF)

Es un marco de trabajo para la creación de aplicaciones orientadas a servicios. Con WCF, es posible enviar datos como mensajes asincrónicos de un extremo de servicio a otro. Un extremo de servicio puede formar parte de un servicio disponible continuamente hospedado por IIS, o puede ser un servicio hospedado en una aplicación. Un extremo puede ser un cliente de un servicio que solicita datos de un extremo de servicio. Los mensajes pueden ser tan simples como un carácter o una palabra que se envía como XML, o tan complejos como una secuencia de datos binarios.

WCF incluye el siguiente conjunto de características:

- Orientación a servicios: Como consecuencia del uso de los estándares de WS, WCF le permite crear aplicaciones orientadas a servicios. SOA, la arquitectura orientada a servicios es el uso de servicios web para enviar y recibir datos. Los servicios tienen la ventaja general de estar débilmente acoplados entre una aplicación y otra en lugar de incluidos en el código. Una relación de acoplamiento débil implica que cualquier cliente creado en cualquier plataforma puede conectar con cualquier servicio siempre y cuando se cumplan los contratos esenciales.
- Interoperabilidad: WCF implementa los estándares del sector, modernos para la interoperabilidad de servicios web.
- Varios modelos de mensajes: Los mensajes se intercambian mediante uno de los distintos modelos. El más común es el de solicitud/respuesta, en que un extremo solicita datos de otro extremo. Y el otro extremo responde. Existen otros modelos, como un mensaje unidireccional, en que un único extremo envía un mensaje sin esperar ninguna respuesta. Un modelo más complejo es el modelo de intercambio dúplex donde dos extremos establecen una conexión y envían datos hacia delante y hacia atrás, similar a un programa de mensajería instantánea. Para obtener más información sobre cómo implementar diferentes modelos de intercambio de mensajes mediante WCF.
- Metadatos de servicios: WCF admite la publicación de metadatos de servicios utilizando los formatos especificados en los estándares de la industria, como WSDL, Esquemas XML y WS-Policy. Estos metadatos pueden utilizarse para generar y configurar automáticamente clientes para el acceso a los servicios de WCF. Los metadatos se pueden publicar sobre HTTP y HTTPS, o utilizando el estándar Intercambio de metadatos de servicios web.
- Contratos de datos: Dado que WCF se basa en .NET Framework, también incluye métodos con código sencillo para proporcionar los contratos que desea aplicar. Uno de los tipos de contrato universales es el contrato de datos. Básicamente, mientras se escribe el código del servicio usando Visual C# o Visual Basic, la forma más sencilla de controlar los datos consiste en crear clases que representan una entidad de datos con propiedades que pertenecen a la misma. WCF incluye un completo sistema para trabajar con datos de esta manera fácil. Cuando se han creado las clases que representan los datos, el servicio genera automáticamente los metadatos que permiten a los clientes ajustarse a los tipos de datos que se han diseñado.
- Seguridad: Es posible cifrar los mensajes para proteger la privacidad, así como obligar a los usuarios a que se autentiquen antes de permitirles recibir mensajes. La seguridad puede implementarse utilizando estándares conocidos como SSL o WS-SecureConversation.
- Varios transportes y codificaciones: Los mensajes pueden enviarse con cualquiera de los protocolos y codificaciones integrados. La combinación más

frecuente de protocolo y codificación consiste en enviar mensajes SOAP codificados de texto utilizando el Protocolo de transferencia de hipertexto (HTTP) usado en World Wide Web. WCF también le permite enviar mensajes sobre TCP, canalizaciones con nombre o MSMQ. Estos mensajes pueden codificarse como texto o utilizando un formato binario optimizado. Los datos binarios pueden enviarse de manera eficaz utilizando el estándar MTOM. Si ninguno de los transportes o codificaciones proporcionados satisface sus necesidades, puede crear uno personalizado.

- Mensajes confiables y en cola: WCF admite intercambio de mensajes confiable usando sesiones confiables implementadas sobre mensajería WS-Reliable y mediante MSMQ.
- Mensajes duraderos: Un mensaje duradero es aquel que nunca se pierde debido a una interrupción de la comunicación. Los mensajes que forman parte de un modelo de mensajes duraderos siempre se guardan en una base de datos. Si se produce una interrupción, la base de datos le permite reanudar el intercambio de mensajes cuando se restablezca la conexión. También puede crear un mensaje duradero utilizando Windows Workflow Foundation (WF).
- Transacciones: WCF también admite las transacciones que usan uno de los tres modelos de transacción: las transacciones WS-Atomic, las API del espacio de nombres System.Transactions y Coordinador de transacciones distribuidas de Microsoft.
- Compatibilidad con AJAX y REST: REST es un ejemplo de una tecnología de la Web 2.0 en evolución. WCF se puede configurar para procesar datos XML "sin formato" que no se ajustan en un sobre SOAP. WCF también se puede extender para admitir formatos XML concretos, como ATOM (un estándar popular de RSS), e incluso formatos no XML, como notación de objetos JavaScript (JSON).
- Extensibilidad: La arquitectura de WCF tiene varios puntos de extensibilidad. Si se necesita una función adicional, existen una serie de puntos de entrada que le permiten personalizar el comportamiento de un servicio.

E. Boot strap 3.0

- Bootstrap se puede descargar de dos maneras, compilado o mediante el código fuente original. Dependiendo de la forma que se haya elegido, se verá una estructura de directorios u otra. En esta sección se muestran los detalles de cada una de ellas. Todos los plugins JavaScript de Bootstrap requieren la librería jQuery para funcionar.

F. jQuery 1.11.2

jQuery UI es una biblioteca de componentes para el framework jQuery que le añaden un conjunto de plug-ins, widgets y efectos visuales para la creación de aplicaciones web. Cada componente o módulo se desarrolla de acuerdo a la filosofía de jQuery Contiene las funciones básicas para el resto de módulos.

Interacciones: Añade comportamientos complejos a los elementos:

- Draggable: Hace al elemento arrastrable.
- Droppable: Permite que el elemento responda a elementos arrastrables.
- Resizable: Permite redimensionar el elemento.
- Selectable: Permite seleccionar entre una lista de elementos.
- Sortable: Ordena una lista de elementos.
- Ziseable: Permite seleccionar el tamaño de los elementos.

Widgets: Es un conjunto completo de controles UI. Cada control tiene un conjunto de opciones configurables y se les pueden aplicar estilos CSS

Efectos**:** Una API para añadir transiciones animadas y facilidades para interacciones.

G.IIS Microsoft Internet Information services

Internet Information Services o IIS1 es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.2

VIII. Sistema para la implementación, mantenimiento y monitoreo de un SGSI para la Universidad Don Bosco

El sistema, abreviado como "SGSI UDB", provee a los usuarios una herramienta que permite visualizar los requerimientos necesarios para cumplir con la norma ISO27001:2005, además de poder definir y gestionar los controles como buenas prácticas conforme a la norma ISO27002, proporcionando a su vez, portabilidad al permitir el acceso al mismo desde diversos dispositivos (Computadoras de escritorio, laptops y dispositivos móviles.).

A. Arquitectura del sistema

El sistema está basado en una arquitectura en 3 capas, como se muestra en el siguiente diagrama*:*

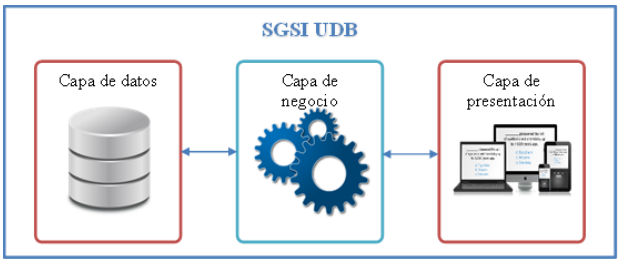

Diagrama 1: Arquitectura del sistema SGSI UDB.

Capa de datos: Es en donde se encuentran almacenados los datos, en esta capa se encuentra la base de datos del sistema y el gestor de la misma.

Capa de negocio: Esta capa incluye todos los cálculos, definición de procesos y validaciones necesarias sobre la capa de datos, como resultado de las solicitudes enviadas desde la capa de presentación. En la capa de negocio se encuentran, además, las librerías y clases utilizadas por el sistema, así como las funciones definidas en el servicio WCF (Windows Communication Fundation) que reciben las solicitudes y muestra los resultados en formato XML, permitiendo, de esta manera la compatibilidad con los modelos de interfaz (web y Windows). [10]

Capa de presentación: Es la interfaz de usuario del sistema, en ella se capturan los datos necesarios para su procesamiento y se muestran los resultados del mismo. En esta capa está definido el sitio web desde el cual se envían las solicitudes y se muestran los resultados, los cuales pueden ser accedidos desde diversos tipos de dispositivos.

B. Seguridad del sistema

El sistema cuenta con diversos mecanismos de seguridad, detallados a continuación: desde cifrado de información sensible, funcionalidades de seguridad sobre la interfaz web y controles de la misma, seguridad a nivel de base de datos, gestión de roles de usuarios, generación de tokens y verificación de direcciones IP, entre otros.

Seguridad en base de datos: Además de tener usuarios específicos para las conexiones a la base de datos, la comunicación y el envío de inserciones, actualizaciones y eliminación de registros es mediante procedimientos almacenados, minimizando, de esta manera, el riesgo del sistema a sufrir ataques utilizando el método SQL Injection.

Gestión de roles de usuarios: Los usuarios del sistema son asignados a 2 roles principales:

- Administrador: El rol de administrador permite la creación de cuentas de usuario y el acceso a mantenimientos de los catálogos del sistema, acceso a funcionalidades como mantenimiento de controles, frecuencia de controles, mantenimiento de activos y sus riesgos, calendarización de auditorías y gestión de requerimientos de la norma ISO 27001 y sus buenas practicas estipuladas en la norma ISO 27002.

- Auditor: Rol específico para el uso general del sistema, no cuenta con los privilegios ni accesos con los que cuenta el rol de administrador, sin embargo, puede acceder a funcionalidades como la evaluación, análisis y tratamiento de riesgo, revisión de activos, riesgos y controles, además de la visualización de auditorías pendientes.

Clase de seguridad "SGSISecurityClass": Para asegurar la confidencialidad de datos se consideran sensibles y que son gestionados por el sistema y realizar actividades de asignación y verificación de tokens, se cuenta con una clase a la medida llamada SGSISecurityClass, la cual contiene los métodos de cifrado y descifrado de datos utilizando el algoritmo AES con un largo de llave de 128 bits; contiene además, otros métodos como lo son la generación de tokens, verificación de combinaciones de tokens y direcciones IP de los usuarios que envían solicitudes al servicio WCF y métodos para la generación de cadenas HASH.

Seguridad en la interfaz de usuario: El sistema cuenta con un sistema de acceso a las herramientas y módulos del mismo, mediante una pantalla de login en la que se realiza, además la

verificación del rol del usuario que pretende acceder al sistema, la cual se muestra en la figura siguiente:

Figura 1: Pantalla de acceso al sistema.

La asignación de roles de los usuarios al sistema se realiza durante la creación y gestión de usuarios del mismo, como lo muestra la figura siguiente:

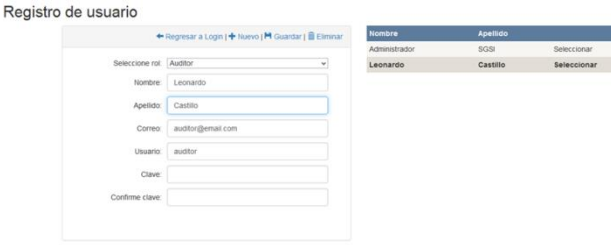

Figura 2: Pantalla de gestión de cuentas de usuarios.

El sistema también cuenta con la verificación de cadenas de caracteres ingresadas por los usuarios del mismo, así como la generación de datos de salida del sistema mediante la clase System.Web.HttpUtility, la cual cuenta con los métodos HTMLEncode y HTMLDecode para la verificación y mapeo de caracteres considerados como especiales en el formato HTML; evitando de esta manera, el ingreso de código HTML malicioso, mediante el método XSS (Cross Site Scripting).

C. Módulos del sistema

Una vez el usuario haya accedido al sistema, dependiendo del rol al que este asignado, se encontrará con la pantalla principal, la cual contiene los módulos presentes en el sistema, mostrando una breve descripción de los mismo y los accesos a las diversas funcionalidades de cada módulo, de la misma forma, el usuario, dependiendo siempre del rol asignado, puede acceder a dichas funcionalidades desde el menú principal del sistema. El diseño de la página principal se muestra en las figuras siguientes:

Figura 3: Pantalla principal del sistema.

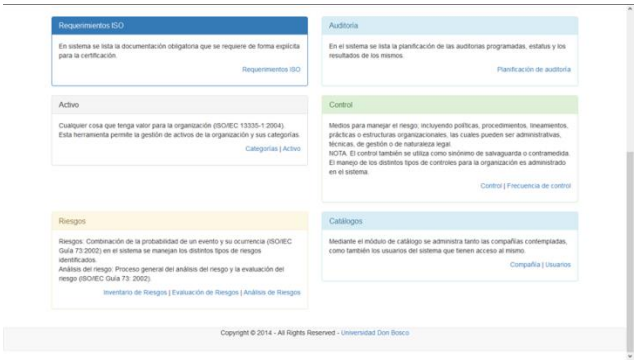

Figura 4: Presentación de los módulos del sistema, con una breve descripción de cada uno de ellos.

Requerimientos ISO: Al acceder a este módulo, se mostrará un listado de los requerimientos mandatorios requeridos de manera explícita para la certificación ISO 27001, en esta pantalla se puede subir o tener acceso a los documentos requeridos por la norma y acceder a interfaces, para verificar la existencia de registros que validen el requerimiento accedido. [11] El diseño de la pantalla es mostrado en la figura a continuación:

Figura 5: Verificación de cumplimiento de requerimientos ISO 27001.

C.1 Catálogos

El módulo de catálogos cuenta con los mantenimientos generales del sistema, como lo son los listados a continuación:

Compañía: Información general de la compañía desde esta pantalla se puede tener acceso a la gestión de áreas de la compañía y a la gestión de personal de la misma.

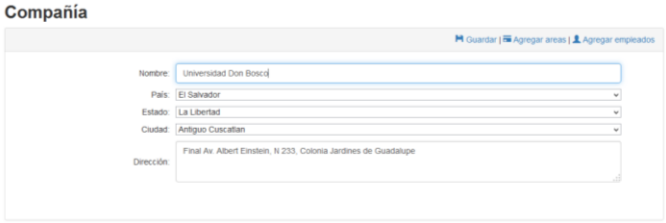

Figura 6: Pantalla de gestión de datos de la compañía.

Áreas de la compañía: En esta pantalla se realiza la gestión de las áreas de la compañía.

Figura 7: Pantalla de gestión de áreas de la compañía.

Personal de la compañía: En esta pantalla se gestiona la información del personal de la compañía, así como la asignación del personal que será dueño de datos.

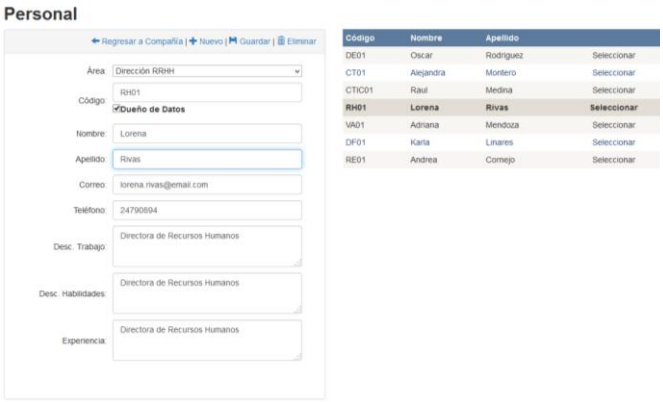

Figura 8: Pantalla de gestión de personal de la organización.

C.2 Activos

Este módulo contiene funcionalidades para la gestión de catálogos de activos y categorías.

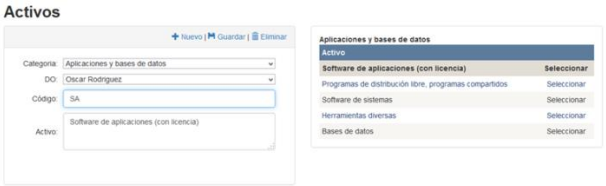

Figura 9: Pantalla de gestión de activos de la organización.

C.3 Controles

Este módulo permite la gestión de las medidas necesarias para el tratamiento del riesgo mediante la presentación de la pantalla Controles, además de gestionar la frecuencia de aplicación de dichos controles. Los diseños de dichas pantallas se muestran a continuación:

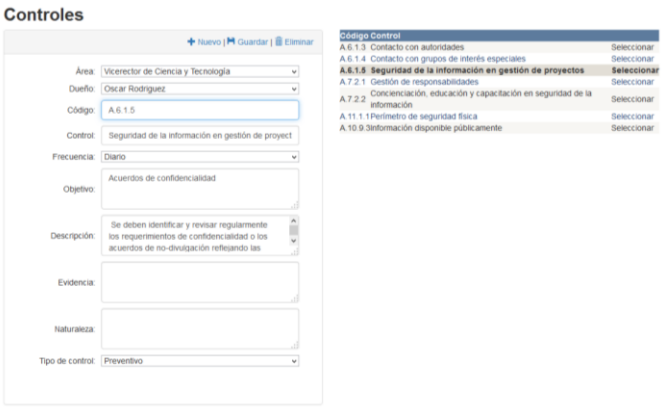

Figura 11: Pantalla de gestión de controles

Figura 12: Pantalla de gestión de frecuencia de controles.

C.4 Riesgos

Este módulo permite a la organización gestionar los registros de riesgos sobre los activos de la misma, realizar evaluaciones de riesgos, generar análisis de riesgos y gestionar cada riesgo incluyendo además, la asignación de controles. Al realizar el tratamiento de riesgo se puede seleccionar las posibles acciones a tomar para el tratamiento del mismo, entre las que se encuentran:

- Transferir: Se comparte el riesgo con un tercero.
- Mitigar: Se asigna uno o varios controles al riesgo.
- Aceptar: La administración esta consiente de que es mayor el beneficio que el riesgo, por tanto el riesgo se encuentra entre los niveles aceptados por la organización.
- Evitar: Dejar de realizar los procedimientos que han sido identificados como desencadenantes del riesgo.

Las pantallas que contienen dichas funcionalidades se presentan a continuación:

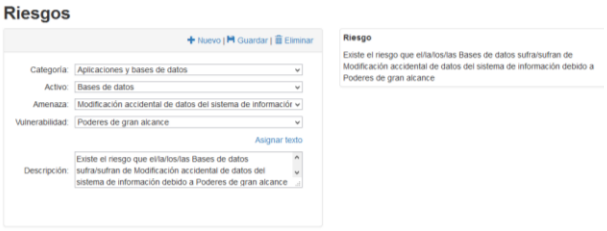

Figura 13: Pantalla de mantenimiento de catálogo de riesgos.

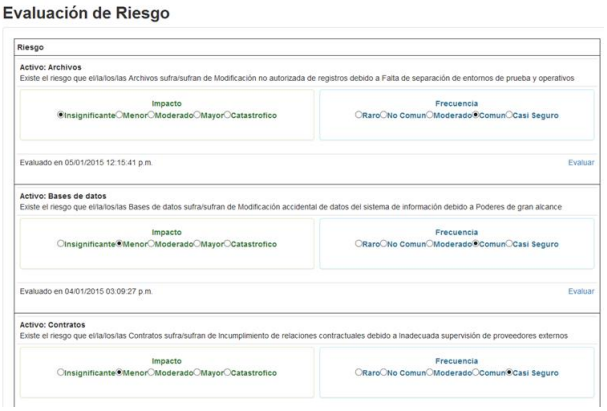

Figura 14. Pantalla de evaluación de riesgos.

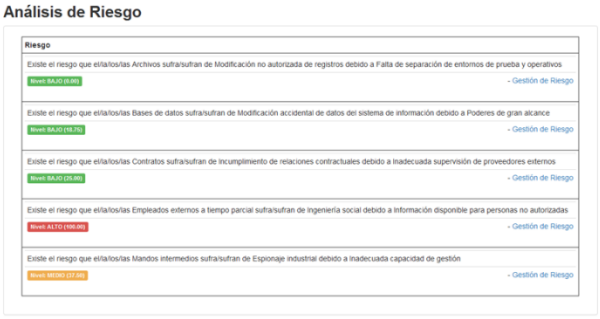

Figura 15: Pantalla de análisis de riesgos.

Figura 16: Pantalla de tratamiento de riesgo y asignación de controles sobre el riesgo.

C.5 Auditoria

En este módulo se realizan las planificaciones de las revisiones de cumplimiento sobre el Sistema de Gestión de la Seguridad de la Información, asignando además los auditores que estarán incluidos en las revisiones y las áreas a las que se realizarán dichas evaluaciones. El diseño de la pantalla se muestra a continuación:

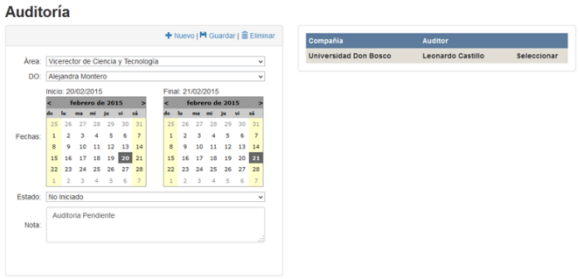

Figura 17: Pantalla de gestión de auditorías sobre el cumplimiento del SGSI.

IX. Conclusiones

1) La implementación de los controles, es un proceso selectivo que requiere de personal de conocimiento en el manejo de la información de su respectiva área y un enfoque en la seguridad de la información.

2) La generación del riesgo se basa en la combinación de las descripciones de la vulnerabilidad con alguna de las posibles amenazas hacia los activos identificados.

3) La evaluación del riesgo sobre un activo incluye la medición cualitativa de la frecuencia y el nivel de impacto de riesgo.

4) La implementación del tratamiento de un riesgo, incluye evitar el riesgo, aceptar el riesgo como un riesgo no influyente en los procesos de la lógica del negocio o transferir el riesgo a un tercero o mitigar el riesgo mediante la selección de uno o varios controles

X. Referencias

[1] (UNE-ISO/IEC 17799:2002 Tecnología de la Información - Técnicas de Seguridad - Código para la práctica de la gestión de la seguridad de la información, 2005).

[2] Guía Oficial Completa (ISC)2 para el CISSP CBK, Tercera Edición.

[3] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, Disponible en línea: http://www.iso27001security.com/html/27001.html. Verificado, Enero 2015.

[4] ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information

security controls, Disponible en línea:
http://www.iso27001security.com/html/27002.html. Verificado, Enero 2015.

[5] (ISO/IEC 27001:2005 Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información - Requerimientos, 2005).

[6] (2012). IT Governance: an International Guide to Data Security and ISO27001/ISO27002, Alan Calder & Steve Watkins, Kogan Page Publishing , Quinta Edición, 2012.

[7] Así es Microsoft Visual Studio. Net, Madrid, España: MCGRAW HILL, 2001.

[8] SQL Server 2008, Francisco Charte Ojeda, 2009.

[9] Desarrollo de Aplicaciones WEB con ASP. NET 2.0, Antonio Martín Sierra, 2007.

[10] Windows Server 2008: Guía del Administrador, William R. Stanek. 2008.

[11] ISO/IEC 27001 - Information security management, Disponible en línea:
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. Verificado, Enero 2015.

Acerca de los Autores.

Castillo Perla, Leonardo J. (Santa Ana, 20 de Noviembre de 1982); Ingeniero en Sistemas Informáticos de la Universidad Católica de El Salvador y egresado de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco.
Actualmente desempeñándose como Auditor de Sistemas Informáticos en Avianca. Experiencia de siete años en auditorias informáticas en múltiples industrias y diversos sectores.

Flores Rivera, Henrry B. (Ciudad Delgado, 9 de agosto de 1977); Ingeniero en Ciencias de la Computación de la Universidad Don Bosco y egresado de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la misma universidad.
Actualmente desempeñándose como Director de Tecnología del Centro de Estudios de Postgrados de la Universidad Don Bosco. Experiencia en el área de tecnología desde catorce años y experiencia docente de ocho años.

Rodriguez Umaña, Oscar A. (Santa Ana, 20 de Febrero de 1985); Ingeniero en Sistemas Informáticos de la Universidad Católica de El Salvador y egresado de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco.
Actualmente desempeñándose como Programador Senior en Enterprise Database El Salvador. Experiencia de ocho años en desarrollo de aplicaciones.

XI. APÉNDICE 1

Figura 18: Diagrama RE Modulo de gestión de riesgo.

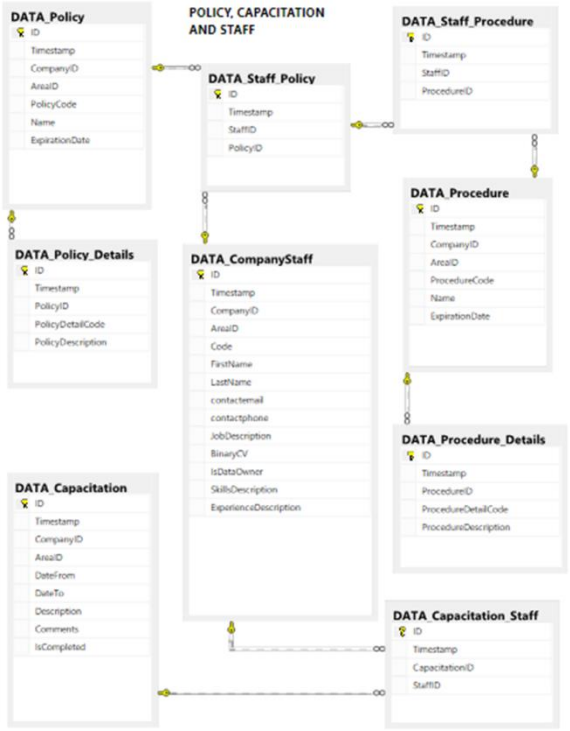

Figura 19: Diagrama RE Gestión de Catálogos

Figura 20: Diagrama RE Gestión de roles de usuario y Auditorías del SGSI.

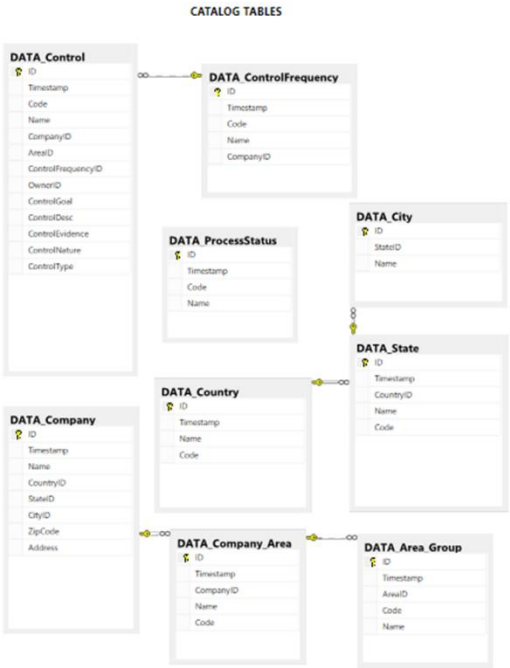

Figura 21: Diagrama RE Gestión de Catálogos y Controles