UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TEMA:

ESTABLECIMIENTO Y DISEÑO DE LOS ENTREGABLES PARA LA IMPLEMENTACIÓN DE LA NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2013

TRABAJO PRÁCTICO DEL EXAMEN COMPLEXIVO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR:

OBACO SISALIMA CHRISTIAN ALBERTO

MACHALA - EL ORO

CESIÓN DE DERECHOS DE AUTOR

Yo, OBACO SISALIMA CHRISTIAN ALBERTO, con C.I. 0603966052, estudiante de la carrera de INGENIERÍA DE SISTEMAS de la UNIDAD ACADÉMICA DE INGENIERÍA CIVIL de la UNIVERSIDAD TÉCNICA DE MACHALA, en calidad de Autor del siguiente trabajo de titulación ESTABLECIMIENTO Y DISEÑO DE LOS ENTREGABLES PARA LA IMPLEMENTACIÓN DE LA NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2013

- Declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional. En consecuencia, asumo la responsabilidad de la originalidad del mismo y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto, asumiendo la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera EXCLUSIVA.

- Cedo a la UNIVERSIDAD TÉCNICA DE MACHALA de forma NO EXCLUSIVA con referencia a la obra en formato digital los derechos de:

  a. Incorporar la mencionada obra al repositorio digital institucional para su democratización a nivel mundial, respetando lo establecido por la Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0), la Ley de Propiedad Intelectual del Estado Ecuatoriano y el Reglamento Institucional.

  b. Adecuarla a cualquier formato o tecnología de uso en internet, así como incorporar cualquier sistema de seguridad para documentos electrónicos, correspondiéndome como Autor(a) la responsabilidad de velar por dichas adaptaciones con la finalidad de que no se desnaturalice el contenido o sentido de la misma.

Machala, 18 de noviembre de 2015

OBACO SISALIMA CHRISTIAN ALBERTO

C.I. 0603966052

1.- INTRODUCCIÓN

La seguridad informática es un proceso que busca establecer mecanismos para conservar en primera instancia la confidencialidad, integridad y disponibilidad de la información, considerando a ésta como el activo con mayor importancia que poseen las organizaciones. Los mecanismos definidos buscan proteger la información contra ataques como *phishing*, ingeniería social, troyanos, *pharming*, entre otros que buscan vulnerar sistemas de información con el fin de robar, destruir, secuestrar o alterar la información y con ello afectar el cumplimiento de las metas del negocio. (SERRANO, 2010)

Dentro de los mecanismos definidos para la protección de la información se pueden establecer: procedimientos que desemboquen en políticas de seguridad, entre otras actividades asociadas, sin obviar la importancia de establecer un marco que permita brindar un orden y orientar los esfuerzos que se hagan en materia de seguridad de la información, propendiendo a que estos apoyen y no ralenticen el desarrollo de los procesos de negocio.

La utilización de un modelo de políticas y procedimientos alineados a la norma ISO/IEC 27002:2013 para la gestión de la Seguridad de la Información, facilitará un cambio socio-cultural con responsabilidad y eficacia en los Departamentos de T.I.

El aumento de las amenazas en contra de la información que circula en las redes locales se multiplican, y aún en nuestro medio todavía no se ha creado una conciencia del riesgo que implica mantener redes desprotegidas, peor aún de disponer de las políticas de seguridad informática que norman los departamentos de T.I, para que así se eviten cuantiosas pérdidas económicas.

2. DESARROLLO

2.1 MARCO TEÓRICO

A continuación se explicarán algunos términos y conceptos para lograr un mejor entendimiento del problema que se abordará en el presente trabajo:

2.1.1 INFORMACIÓN

La norma ISO/IEC 27002 la define como un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. (INFOSEC, 2000)

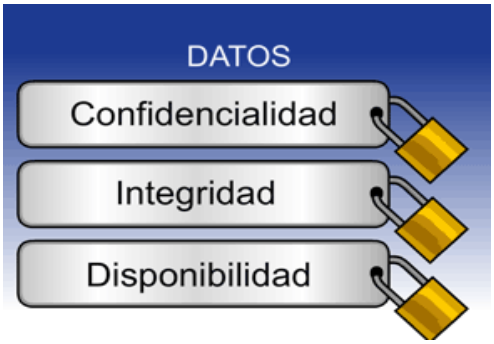
2.1.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. (CORE ONE IT, 2014)

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. (CORE ONE IT, 2014)

Ilustración 1: Principios Básicos de la Seguridad de la Información



Fuente (ISMS Forum Spain, 2011)

2.1.3 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los requerimientos de seguridad de la información de una organización pueden salir de tres fuentes. Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la

evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial. Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural. Finalmente la última fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones. (Prada, 2009)

2.1.4 FAMILIA ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). (ISO 27000, 2012)

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen:

ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.

ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005, su versión más reciente fue publicada en el 2013.

ISO/IEC 27002 - *Information technology - Security techniques - Code of practice for information security management*. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Su versión más reciente fue publicada en el 2013.

ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre de 2009.

ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.

ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

ISO/IEC 27007 - Es una guía para auditar al SGSI. Se encuentra en preparación.

ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

2.1.5 ISO/IEC 27002:2013

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)". (DIANA, MARTÍN, & MANUEL, 2011)

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. Políticas de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Seguridad ligada a los Recursos Humanos.
4. Gestión de los Activos.
5. Control de Accesos.
6. Criptografía.
7. Seguridad Física y Ambiental.
8. Seguridad de las Operaciones
9. Seguridad de las Comunicaciones.
10. Adquisición de sistemas, desarrollo y mantenimiento de los sistemas de información.
11. Relaciones con los Proveedores.
12. Gestión de Incidencias que afectan a la Seguridad de la Información:
13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
14. Cumplimiento (Gabriela2409, 2015)

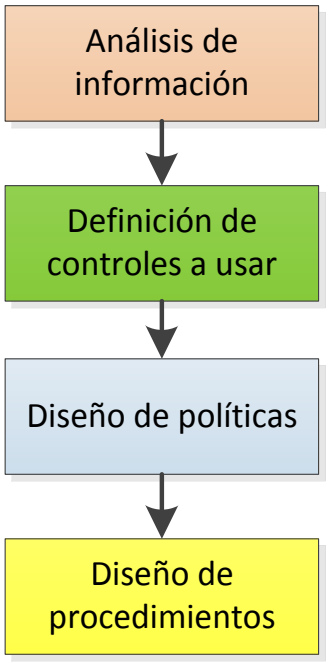
Ilustración 2: Pirámide de Clasificación de Documentos

Fuente (iso27000.es, 2012)

2.2 MARCO METODOLÓGICO

La Figura 3 muestra las fases que se seguirán para el desarrollo del presente proyecto.

Ilustración 3: Metodología Implementada



La siguiente tabla muestra las actividades y entregables propuestos para cada uno de los objetivos específicos del trabajo practico, así como las materias relacionadas, herramientas y fuentes de información usadas para cada uno de ellos.

Tabla 1. Actividades y Entregables Propuestos

OBJETIVO	FASE	ACTIVIDADES	ENTREGABLES	HERRAMIENTAS Y FUENTES
1. Estudiar y analizar la problemática de la seguridad de la información en la organización	**ANÁLISIS DE INFORMACIÓN**	• Revisar de literatura y documentación relacionada con la norma ISO/IEC 27002. • Revisar la documentación existente de los procesos del departamento de TI • Identificar las necesidades de seguridad de la empresa	• Marco teórico relacionado con la problemática. • Informe de necesidades de seguridad de la empresa.	• Documentación relacionada con la norma ISO/IEC 27002. • Documentación existente de los procesos del departamento de TI • Entrevistas a usuarios
2. Efectuar el diagnóstico de los riesgos de seguridad de la información para determinar los controles que se deben implementar	**DEFINICIÓN DE CONTROLES A UTILIZAR**	• Identificar los riesgos de seguridad de la compañía. • Establecer y aplicar un método para priorizar los riesgos de seguridad de la información en la compañía. • Determinar los controles que se utilizarán para minimizar los riesgos prioritarios	• Lista de controles a aplicar	• Checklist • Cuadros estadísticos • Formato de inspección de riesgos
3. Diseñar y adecuar las políticas, procesos y procedimientos existentes en el área de tecnología en la empresa Leasing Bolívar S.A. para alinearse con la norma	**DISEÑO DE POLÍTICAS**	• Elaborar las políticas de seguridad de la información basadas en la norma ISO/IEC 27002. • Documentar las nuevas políticas de seguridad de la información de la compañía.	• Documento propuesto de políticas de seguridad de la información. • Documentación de los procesos y procedimientos del área de tecnología de la empresa.	• Diagramas de flujo • Organigrama • Descripciones de procesos • Funciones de cargos

ISO/IEC 27002, haciendo uso de controles dentro de dichos procesos o procedimientos.	**DISEÑO DE PROCEDIMIENTOS**	• Identificar los procesos del departamento de TI y determinar en qué estado se encuentran. • Documentar los procedimientos y procesos del departamento de TI de la empresa.		
4. Definir una estructura documental para el sistema de gestión.		• Determinar las estructuras documentales que maneja la compañía. • Escribir el documento del estándar de documentación del nuevo sistema de gestión de la información. • Diseñar plantillas y herramientas de documentación para el sistema de gestión. • Diseñar y documentar un sistema de administración de incidentes de seguridad de la información.	• Documento de estándares de documentación del nuevo sistema de gestión de la información. • Plantillas y herramientas de documentación del sistema. • Documentación del sistema de administración de incidentes de seguridad de la información.	• Investigación bibliográfica • Entrevistas

Fuente: Elaborado por Christian Obaco

2.3 RESULTADOS

En base a la estructura administrativa del departamento de tecnología de la información de la empresa **Ver Anexo 1** se elaboraron y documentaron las políticas de control de acceso las cuales están especificadas en el **Anexo 3** para el cumplimiento del control del control 9.1.1 del dominio de control de accesos.

Los cuestionarios del **Anexo 2** fueron utilizados para determinar la madurez de los procedimientos ad hoc utilizados al momento de realizar la investigación.

Se definió un manual de procedimientos especificado en el **Anexo 4** dentro de los cuales se especifican las funciones y responsabilidades del personal de TI involucrado.

Los formatos utilizados en los procedimientos se pueden encontrar en el **Anexo 5**

Finalmente se hizo un análisis de las herramientas de software que se serían necesarias para la implementación del presente proyecto, documentado en el **Anexo 6** las aplicaciones elegidas.

En la Tabla 2 mostrada a continuación se muestran los códigos de los procedimientos en los que se aplican los controles de seguridad requeridos por la norma.ISO/IEC 27002:2013 que están dentro del alcance del presente proyecto.

Se encontró que todos los controles fueron aplicables a la empresa, existen controles que no tienen un procedimiento específico los cuales son cubiertos con la política de control de acceso.

Tabla 2 Alineacion de controles y procedimientos

DOMINIO	CONTROL	PROCEDIMIENTO
9. CONTROL DE ACCESOS.	9.1.1 Política de control de accesos.	
	9.1.2 Control de acceso a las redes y servicios asociados.	P 01 TI
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	P 01 TI
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	P 01 TI
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	P 01 TI
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	P 01 TI
	9.2.5 Revisión de los derechos de acceso de los usuarios.	P 02 TI
	9.2.6 Retirada o adaptación de los derechos de acceso	P 01 TI
	9.3.1 Uso de información confidencial para la autenticación.	P 01 TI
	9.4.1 Restricción del acceso a la información.	
	9.4.2 Procedimientos seguros de inicio de sesión.	P 03 TI
	9.4.3 Gestión de contraseñas de usuario.	
	9.4.4 Uso de herramientas de administración de sistemas.	

	9.4.5 Control de acceso al código fuente de los programas	P 03 TI
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	14.1.1 Análisis y especificación de los requisitos de seguridad.	P 03 TI
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	P 03 TI
	14.1.3 Protección de las transacciones por redes telemáticas	P 03 TI
	14.2.1 Política de desarrollo seguro de software.	P 03 TI
	14.2.2 Procedimientos de control de cambios en los sistemas.	P 03 TI
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el	P 03 TI
	Sistema operativo.	P 03 TI
	14.2.4 Restricciones a los cambios en los paquetes de software.	P 03 TI
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	P 03 TI
	14.2.6 Seguridad en entornos de desarrollo.	P 03 TI
	14.2.7 Externalización del desarrollo de software.	P 03 TI
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	P 03 TI
	14.2.9 Pruebas de aceptación.	P 03 TI
	14.3.1 Protección de los datos utilizados en pruebas.	P 03 TI
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1.1 Responsabilidades y procedimientos.	P 04 TI
	16.1.2 Notificación de los eventos de seguridad de la información.	P 04 TI
	16.1.3 Notificación de puntos débiles de la seguridad.	P 04 TI
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	P 04 TI
		P 04 TI
	16.1.5 Respuesta a los incidentes de seguridad.	P 04 TI
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	P 04 TI
	16.1.7 Recopilación de evidencias	P 04 TI

Fuente: (ESPAÑOL, 2005)
Investigado por: Christian Obaco

3.- CONCLUSIONES

Cumpliendo con el alcance planteado en este proyecto de investigación, se analizaron las políticas para los siguientes dominios: Control de Acceso, Adquisición, Desarrollo y Mantenimiento de Sistemas de Información y Gestión de Incidentes de la Seguridad de la Información.

Es necesario definir los responsables de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan vacíos ni problemas de definiciones claras de responsabilidades.

El cumplimiento de las políticas desarrolladas no garantiza que no se pueda sufrir un ataque informático, pero se minimizará en gran medida los riesgos asociados a los activos de información limitando el alcance y el impacto del ataque.

No se requiere mayor inversión en compra de tecnología para la aplicación de los controles analizados, la mayoría de cambios propuestos se basan en el cambio de procedimientos y metodologías de trabajo.

El éxito de la implementación del proyecto dependerá en gran medida del nivel de concientización de los usuarios tanto del personal técnico como del usuario final. Es necesario realizar campañas de concientización permanentes para recordar al recurso humano la importancia de la correcta manipulación de la información en el día a día.

URKUND

Urkund Analysis Result

Analysed Document: Informe Final Christian Obaco.docx (D16367676)
Submitted: 2015-11-24 21:51:00
Submitted By: caos1988@gmail.com
Significance: 9 %

Sources included in the report:

TesisCompletaEly.docx (D14122788)
https://es.wikipedia.org/wiki/OWASP_Top_10
https://es.wikipedia.org/wiki/ISO/IEC_27000-series
https://es.wikipedia.org/wiki/Seguridad_de_la_informacion
http://www.iso27000.es/download/ControlesISO27002-2013.pdf
http://www.iso27000.es/iso27002_14.html
http://compromiso.sena.edu.co/documentos/docs_pdf/1391442264_GTI-P-002_Procedimiento_Gestion_de_los_Sistemas_de_informacion.xlsx.pdf
https://seguridadpcs.wordpress.com/recomendaciones-2/otros-softwares/administradores-de-contrasenas/
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Instances where selected sources appear:

16

Ing. Wilmer Braulio Rivas Asanza
C.I 0702580192