PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001: 2005

ORGANIZACION UNIVERSITARIA

TRABAJO FINAL DE MASTER

Elaborado por: LORENA SUAREZ SIERRA

MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC (MISTIC)

JUNIO 2013

INDICE

INTRODUCCION

La utilización de la tecnología de la información y las comunicaciones ha permitido a las empresas ampliar su cobertura en servicios y hacerla cada día más competitivas, ofreciéndoles a sus clientes una gran gama de posibilidades para acceder a ellos. Así mismo las TIC, han permitido que las empresas lleven de manera remota los procesos administrativos así como la comunicación entre sus empleados necesarios para su funcionamiento. En este sentido, las facilidades de comunicación para las empresas de hoy, las ha conllevado a ser más vulnerables o atacadas por cualquier persona que tenga el conocimiento o tal vez por una organización delincuencial que utiliza diferentes herramientas tecnológicas para afectar a sus víctimas y obtener beneficios.

El mismo servicio en la web que las empresas de hoy presta a sus clientes, los ha afectado a ellos de alguna manera, por cuanto a través de los pagos en línea que han realizado para la compra de servicios, consultas, actualización de datos, entre otros son aprovechados también por los delincuentes para acceder a sus claves o contraseñas, a sus computadoras personales para copia y/o eliminación de su información entre otras. Lo anterior hace que de alguna forma, los clientes se nieguen a realizar transacciones a través de estos medios de comunicación masiva como internet perdiendo las organizaciones posibles clientes potenciales a nivel mundial. En este orden las empresas deben garantizar a sus clientes una transacción protegida, así como las orientaciones pertinentes para evitar fraudes internauticos.

En concordancia con la necesidad de las empresas de asegurar su información además de sus dispositivos computacionales y de comunicación, de manera organizada, sistemática, documentada y conocida, que involucre todos los aspectos físicos, lógicos y humanos de la organización. ISO como organización Internacional de Estándares, ha definido el estándar ISO 27001 para La gestión de la seguridad de la información anunciando *: "El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías".* *http://www.iso27000.es/sgsi.html.*

Con el desarrollo de este trabajo se presenta el establecimiento de las bases para implementación de un Sistema de Gestión de la Seguridad de la Información SGSI con las normas de la ISO/IEC 27001:2005 en una empresa real, quién proporcionará todos los insumos y colaboración necesaria para el desarrollo del

proyecto, lo cual redundará en su beneficio. Para la coherencia y organización del trabajo, se desarrollará en 6 fases secuenciales así: fase 1: Situación actual, fase 2: Sistema de gestión documental, fase 3: Análisis de riesgos, fase 4: Plan de tratamiento de riesgos y fase 5: Auditoría de cumplimiento.

Preámbulo "Las normas ISO/IEC 27000"

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotenía, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, asì como públicas y privadas.

A continuación se relacionan en la siguiente tabla No. 3, la temática que define cada norma.

Tabla No. 3 Relación de serie de las normas ISO/IEC 27000

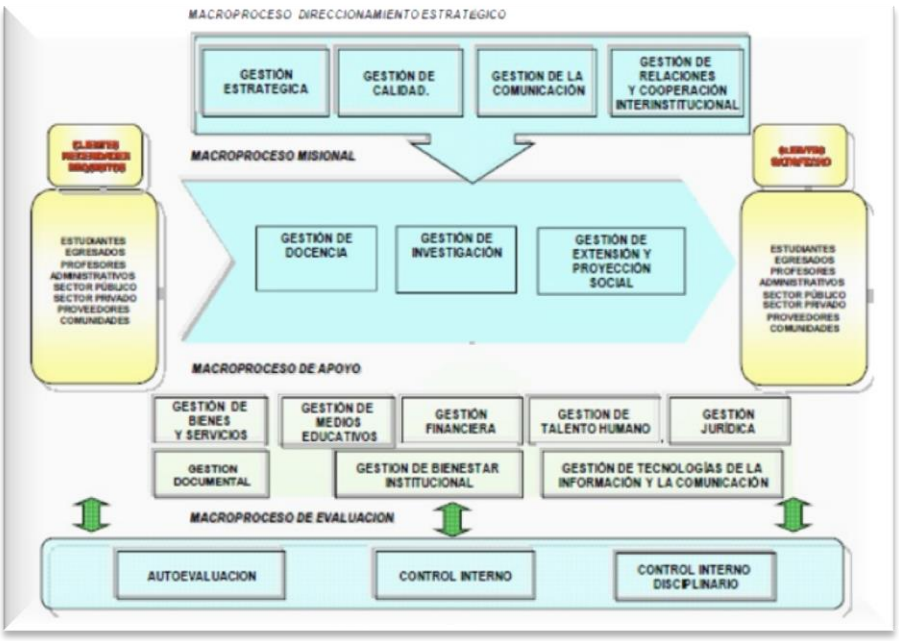
Normas	Temática
ISO 27000	Gestión de la seguridad de la información (Fundamentos y vocabulario)
ISO 27001	Especificaciones para un SGSI
ISO 27002	Código de buenas prácticas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistema de métricas e indicadores
ISO 27005	Guía de análisis y gestión de riesgos
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.
ISO/IEC TR 27008:	Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI
ISO/IEC 27010:	Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

1. FASE 1: SITUACION ACTUAL. CONTEXTUALIZACION, OBJETIVOS Y ANALISIS DIFERENCIAL

Descripción y entorno de la actividad de la empresa

La empresa seleccionada para la implementación de la ISO/IEC 27001:2005, es una universidad de formación de pregrado y postgrado de modalidad presencial de orden regional. Posee una estructura jerárquica, donde el rector es la máxima autoridad después del consejo superior, quién es el encargado de la toma de decisiones importantes que involucren aspectos presupuestales, reorganización o cambios estructurales de la institución, creación de nuevos programas de formación, proyectos de inversión entre otras. La universidad posee dos sedes, donde ofrece sus programas, ubicados en ciudades diferentes. La empresa se encuentra organizada operativamente a través del modelo por procesos, la cual se esquematiza en el gráfico 1.

Grafico No. 1 Organización por mapa de procesos



Por ser una entidad universitaria sus clientes son los estudiantes matriculados en los diferentes programas de formación de pregrado y postgrado que actualmente ofrece con 12.285 estudiantes en una sede y en la otra sede 645 estudiantes en pregrado y 35 estudiantes en postgrado. También posee empleados académicos y administrativos, es decir, académicos como el personal docente, que se encarga de la atención estudiantil y algunos procesos académicos y el personal

administrativo encargada de toda la operatividad de la institución que incluye las dependencias de recursos humanos, jurídicos, inventarios, tesorería, contabilidad, entre otros. En la siguiente tabla se encuentra la relación de empleados en las dos áreas anunciadas con un total del 698 empleados. Por el número de empleados que posee la empresa, esta es considerada una empresa mediana

Tabla No. 1 Listado de empleados académicos y administrativos

Tipos de empleados	Número de empleados
Académicos (docentes)	478
Administrativos(funcionarios)	220
Total empleados	**698**

Actualmente la oficina de sistemas es la encargada de administrar, dar soporte, desarrollar sistemas de información y responsabilizarse de toda la infraesctructura tecnológica de la universidad, tiene 5 empleados, únicamente de planta la jefe de sistemas y el otro personal se encuentra por contractos a término fijo muy cortos, lo cual no garantiza el compromiso de parte de los empleados por la preservación y seguridad de los activos que actualmente posee la universidad.

1.2 ANALISIS DIFERENCIAL

Estado inicial de la seguridad

En relación a la evaluación de la aplicabilidad e implementación de los controles de la ISO/IEC 27001 e ISO/IEC 27002, en la empresa, se puede determinar que el sistema de seguridad es *bajo,* ya que a pesar de existen implementados algunos controles, la mayoría no están implementados o medianamente implementados. El nivel de seguridad bajo que actualmente posee la empresa, se puede observar en la evaluación de cada uno de los controles que se realizaron a través de la tabla 2 de Análisis diferencial de la institución.

Tabla No. 2 Análisis diferencial de la empresa seleccionada

Sección	Control	Aplica	Estado	Observaciones
C	**Cláusulas**			
C.4	Sistemas de Gestión de la Seguridad de la Información	No aplica		No aplica
C.5	Responsabilidad de la dirección	No aplica		No aplica
C.6	Auditorías Internas del SG	No aplica		No aplica
C.7	Revisión por la dirección	No aplica		No aplica
C.8	Mejora del SG	No aplica		No aplica
A.5	**POLÍTICA DE SEGURIDAD**			
A.5.1	Política de seguridad de la información			
A.5.1.1	Documento de política de seguridad de la información	Aplica	Parcialmente implementado	Le falta la aprobación
A.5.1.2	Revisión de la política de seguridad de la información	Aplica	Sin implementar	
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**			
A.6.1	Organización interna			
A.6.1.1	Compromiso de la Dirección con la seguridad de la información	Aplica	Sin implementar	Existe desconocimiento
A.6.1.2	Coordinación de la seguridad de la información	Aplica	Sin implementar	
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	Aplica	Parcialmente implementado	Responsabilidades a nivel de seguridad perimetral y control de acceso a SI
A.6.1.4	Proceso de autorización de recursos para el procesado de la información	Aplica	Implementado	PRESUPUESTAL
A.6.1.5	Acuerdos de confidencialidad	Aplica	Parcialmente implementado	Solo implementado parcialmente para contratistas
A.6.1.6	Contacto con las autoridades	Aplica	Parcialmente implementado	Con el equipo forense del CTI
A.6.1.7	Contacto con grupos de especial interés	Aplica	Sin implementar	
A.6.1.8	Revisión independiente de la seguridad de la información	Aplica	Parcialmente implementado	Contratación externa para seguridad perimetral con la firma GLOBALTEK SECURITY
A.6.2	Terceros			
A.6.2.1	Identificación de los riesgos derivados del acceso de terceros	Aplica	Sin implementar	
A.6.2.2	Tratamiento de la seguridad en la relación con los clientes	Aplica	Sin implementar	
A.6.2.3	Tratamiento de la seguridad en contratos con terceros	Aplica	Sin implementar	

A.7	**GESTIÓN DE ACTIVOS**			
A.7.1	Responsabilidad sobre los activos			
A.7.1.1	Inventario de activos	Aplica	Implementado	
A.7.1.2	Propiedad de los activos	Aplica	Implementado	Responsabilidad de activos
A.7.1.3	Uso aceptable de los activos	Aplica	Implementado	
A.7.2	Clasificación de la información			
A.7.2.1	Directrices de clasificación	Aplica	Sin implementar	No existen políticas de clasificación de información
A.7.2.2	Etiquetado y manipulado de la información	Aplica	Sin implementar	
A.8	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**			
A.8.1	Antes del empleo			
A.8.1.1	Funciones y responsabilidades	Aplica	Parcialmente implementado	Solo para recurso humano en planta
A.8.1.2	Investigación de antecedentes	Aplica	Implementado	Procuraduria y contraloría
A.8.1.3	Términos y condiciones de contratación	Aplica	Implementado	Cláusulas de confidencialidad en contratos cuando así es requerido.
A.8.2	Durante el empleo			
A.8.2.1	Responsabilidades de la Dirección	Aplica	Sin implementar	
A.8.2.2	Concienciación, formación y capacitación en seguridad de la información	Aplica	Parcialmente implementado	Sólo para responsable del Centro de Cómputo se ha dado formación y participación en eventos de seguridad informática
A.8.2.3	Proceso disciplinario	Aplica	Sin implementar	
A.8.3	Cese del empleo o cambio de puesto de trabajo			
A.8.3.1	Responsabilidad del cese o cambio	Aplica	Parcialmente implementado	La responsabilidad de notificación es de la Oficina de talento humano
A.8.3.2	Devolución de activos	Aplica	Implementado	Los bienes en delegación se entregan al finalizar un contrato o un nombramiento
A.8.3.3	Retirada de los de derechos de acceso	Aplica	Parcialmente implementado	Para los SI siempre y cuando la Oficina de Informática sea notificada del retiro del funcionario o

				contratista.
A.9	SEGURIDAD FÍSICA Y AMBIENTAL			
A.9.1	**Áreas seguras**			
A.9.1.1	Perímetro de seguridad física	Aplica	Implementado	
A.9.1.2	Controles físicos de entrada	Aplica	Implementado	
A.9.1.3	Seguridad de oficinas, despachos e instalaciones	Aplica	Parcialmente implementado	Algunas oficinas presentan deficiencias
A.9.1.4	Protección contra las amenazas externas y de origen ambiental	Aplica	Implementado	
A.9.1.5	Trabajo en Áreas seguras	Aplica	Implementado	
A.9.1.6	Áreas de acceso público y de carga y descarga	Aplica	Implementado	
A.9.2	**Seguridad de los equipos**			
A.9.2.1	Emplazamiento y protección de equipos	Aplica	Parcialmente implementado	
A.9.2.2	Instalaciones de suministro	Aplica	Sin implementar	
A.9.2.3	Seguridad del cableado	Aplica	Parcialmente implementado	
A.9.2.4	Mantenimiento de los equipos	Aplica	Parcialmente implementado	Limitaciones para el mantenimiento de algunos equipos
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	No aplica		
A.9.2.6	Reutilización o retirada segura de equipos	Aplica	Sin implementar	
A.9.2.7	Retirada de materiales propiedad de la empresa	Aplica	Parcialmente implementado	Existe deficiencias en control de la vigilancia
A.10	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**			
A.10.1	Responsabilidades y procedimientos de operación			
A.10.1.1	Documentación de los procedimientos de operación	Aplica	Parcialmente implementado	
A.10.1.2	Gestión de cambios	Aplica	Parcialmente implementado	
A.10.1.3	Segregación de tareas	Aplica	Parcialmente implementado	
A.10.1.4	Separación de los recursos de desarrollo, prueba y operación	Aplica	Parcialmente implementado	Existe separación de los recursos para desarrollo de software
A.10.2	Gestión de la provisión de servicios por terceros			
A.10.2.1	Provisión de servicios	Aplica	Implementado	
A.10.2.2	Supervisión y revisión de los servicios prestados por terceros	Aplica	Implementado	
A.10.2.3	Gestión de cambios en los servicios prestados por terceros	Aplica	Parcialmente implementado	
A.10.3	Planificación y aceptación del sistema			

A.10.3.1	Gestión de capacidades	Aplica	Sin implementar	
A.10.3.2	Aceptación del sistema	Aplica	Sin implementar	
A.10.4	Protección contra código malicioso y descargable			
A.10.4.1	Controles contra el código malicioso	Aplica	Parcialmente implementado	
A.10.4.2	Controles contra el código descargado en el cliente	Aplica	Parcialmente implementado	Protección con antivirus corporativo y políticas en el firewall
A.10.5	Copias de seguridad			
A.10.5.1	Copias de seguridad de la información	Aplica	Implementado	
A.10.6	Gestión de la seguridad de las redes			
A.10.6.1	Controles de red	Aplica	Parcialmente implementado	
A.10.6.2	Seguridad de los servicios de red	Aplica	Parcialmente implementado	
A.10.7	Manipulación de los soportes			
A.10.7.1	Gestión de soportes extraí-bles	No aplica		
A.10.7.2	Retirada de soportes	No aplica		
A.10.7.3	Procedimientos de manipulación de la información	Aplica	Parcialmente implementado	
A.10.7.4	Seguridad de la documentación del sistema	Aplica	Parcialmente implementado	
A.10.8	Intercambio de información			
A.10.8.1	Políticas y procedimientos de intercambio de información	Aplica	Parcialmente implementado	
A.10.8.2	Acuerdos de intercambio	Aplica	Sin implementar	
A.10.8.3	Soportes físicos en tránsito	Aplica	Parcialmente implementado	
A.10.8.4	Mensajería electrónica	Aplica	Parcialmente implementado	
A.10.8.5	Sistemas de información empresariales	Aplica	Parcialmente implementado	
A.10.9	Servicios de comercio electrónico			
A.10.9.1	Comercio electrónico	Aplica	Implementado	
A.10.9.2	Transacciones en línea	Aplica	Implementado	
A.10.9.3	Información puesta a disposición pública	Aplica	Implementado	
A.10.10	Supervisión			
A.10.10.1	Registro de auditorías	Aplica	Parcialmente implementado	
A.10.10.2	Supervisión del uso del sistema	Aplica	Parcialmente implementado	
A.10.10.3	Protección de la información de los registros	Aplica	Implementado	
A.10.10.4	Registros de administración y operación	Aplica	Sin implementar	
A.10.10.5	Registro de fallos	Aplica	Parcialmente implementado	
A.10.10.6	Sincronización del reloj	Aplica	Implementado	Los servidores tiene la hora

				nacional de Cámara de comercio.
A.11	**CONTROL DE ACCESO**			
A.11.1	Requisitos de negocio para el control de acceso			
A.11.1.1	Política de control de acceso	Aplica	Parcialmente implementado	
A.11.2	Gestión de acceso de usuario			
A.11.2.1	Registro de usuario	Aplica	Implementado	
A.11.2.2	Gestión de privilegios	Aplica	Implementado	
A.11.2.3	Gestión de contraseñas de usuario	Aplica	Implementado	
A.11.2.4	Revisión de los derechos de acceso de usuario	Aplica	Parcialmente implementado	
A.11.3	Responsabilidades de usuario			
A.11.3.1	Uso de contraseña	Aplica	Parcialmente implementado	
A.11.3.2	Equipo de usuario desatendido	Aplica	Sin implementar	
A.11.3.3	Polí-tica de puesto de trabajo despejado y pantalla limpia	Aplica	Parcialmente implementado	
A.11.4	Control de acceso a la red			
A.11.4.1	Política de uso de los servicios en red	Aplica	Parcialmente implementado	
A.11.4.2	Autenticación de usuario para conexiones externas	Aplica	Parcialmente implementado	
A.11.4.3	Identificación de equipos en las redes	Aplica	Implementado	
A.11.4.4	Diagnóstico remoto y protección de los puertos de configuración	Aplica	Parcialmente implementado	
A.11.4.5	Segregación de las redes	Aplica	Parcialmente implementado	
A.11.4.6	Control de la conexión a la red	Aplica	Parcialmente implementado	
A.11.4.7	Control de encaminamiento (routing) de red	Aplica	Parcialmente implementado	
A.11.5	Control de acceso al sistema operativo			
A.11.5.1	Procedimientos seguros de inicio de sesión	Aplica	Implementado	
A.11.5.2	Identificación y autenticación de usuario	Aplica	Implementado	
A.11.5.3	Sistema de gestión de contraseñas	Aplica	Parcialmente implementado	
A.11.5.4	Uso de los recursos del sistema	Aplica	Parcialmente implementado	
A.11.5.5	Desconexión automática de sesión	Aplica	Parcialmente implementado	
A.11.5.6	Limitación del tiempo de conexión	Aplica	Parcialmente implementado	
A.11.6	Control de acceso a las aplicaciones y a la información			
A.11.6.1	Restricción del acceso a la información	Aplica	Implementado	
A.11.6.2	Aislamiento de sistemas sensibles	Aplica	Implementado	
A.11.7	Ordenadores portátiles y teletrabajo			

A.11.7.1	Ordenadores portátiles y comunicaciones móviles	Aplica	Sin implementar	
A.11.7.2	Teletrabajo	No aplica	Sin implementar	
A.12	**ADQUISICIÓN,DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**			
A.12.1	Requisitos de seguridad de los sistemas de información			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Aplica	Parcialmente implementado	
A.12.2	Tratamiento correcto de las aplicaciones			
A.12.2.1	Validación de los datos de entrada	Aplica	Parcialmente implementado	
A.12.2.2	Control del procesamiento interno	Aplica	Parcialmente implementado	
A.12.2.3	Integridad de los mensajes	Aplica	Parcialmente implementado	
A.12.2.4	Validación de los datos de salida	Aplica	Parcialmente implementado	
A.12.3	Controles criptográficos			
A.12.3.1	Política de uso de los controles criptográficos	Aplica	Sin implementar	
A.12.3.2	Gestión de claves	Aplica	Parcialmente implementado	
A.12.4	Seguridad de los archivos de sistema			
A.12.4.1	Control del software en explotación	Aplica	Parcialmente implementado	
A.12.4.2	Protección de los datos de prueba del sistema	Aplica	Parcialmente implementado	
A.12.4.3	Control de acceso al código fuente de los programas	Aplica	Implementado	
A.12.5	Seguridad en los procesos de desarrollo y soporte			
A.12.5.1	Procedimientos de control de cambios	Aplica	Parcialmente implementado	
A.12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Aplica	Parcialmente implementado	
A.12.5.3	Restricciones a los cambios en los paquetes de software	Aplica	Sin implementar	
A.12.5.4	Fugas de información	Aplica	Sin implementar	
A.12.5.5	Externalización del desarrollo de software	Aplica	Parcialmente implementado	
A.12.6	Gestión de la vulnerabilidad técnica			
A.12.6.1	Control de las vulnerabilidades técnicas	Aplica	Sin implementar	
A.13	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**			
A.13.1	Notificación de eventos y puntos débiles de la seguridad de la información			
A.13.1.1	Notificación de los eventos de seguridad de la información	Aplica	Sin implementar	
A.13.1.2	Notificación de puntos débiles de la seguridad	Aplica	Sin implementar	

A.13.2	Gestión de incidentes de seguridad de la información y mejoras			
A.13.2.1	Responsabilidades y procedimientos	Aplica	Sin implementar	
A.13.2.2	Aprendizaje de los incidentes de seguridad de la información	Aplica	Sin implementar	
A.13.2.3	Recopilación de evidencias	Aplica	Sin implementar	
A.14	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**			
A.14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio			
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Aplica	Sin implementar	
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Aplica	Sin implementar	
A.14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	Aplica	Sin implementar	
A.14.1.4	Marco de referencia para la planificación de la continuidad del negocio	Aplica	Sin implementar	
A.14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad	Aplica	Sin implementar	
A.15	**CUMPLIMIENTO**			
A.15.1	Cumplimiento de los requisitos legales			
A.15.1.1	Identificación de la legislación aplicable	Aplica	Parcialmente implementado	
A.15.1.2	Derechos de propiedad intelectual (DPI)	Aplica	Parcialmente implementado	
A.15.1.3	Protección de los documentos de la organización	Aplica	Parcialmente implementado	
A.15.1.4	Protección de datos y privacidad de la información personal	Aplica	Sin implementar	
A.15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	Aplica	Sin implementar	
A.15.1.6	Regulación de los controles criptográficos	Aplica	Sin implementar	
A.15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico			
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	Aplica	Sin implementar	
A.15.2.2	Comprobación del cumplimiento técnico	Aplica	Sin implementar	
A.15.3	Consideraciones de las auditorías de los sistemas de información			
A.15.3.1	Controles de auditoría de los sistemas de información	Aplica	Parcialmente implementado	
A.15.3.2	Protección de las herramientas de auditorí-a de los sistemas de información	Aplica	Parcialmente implementado	

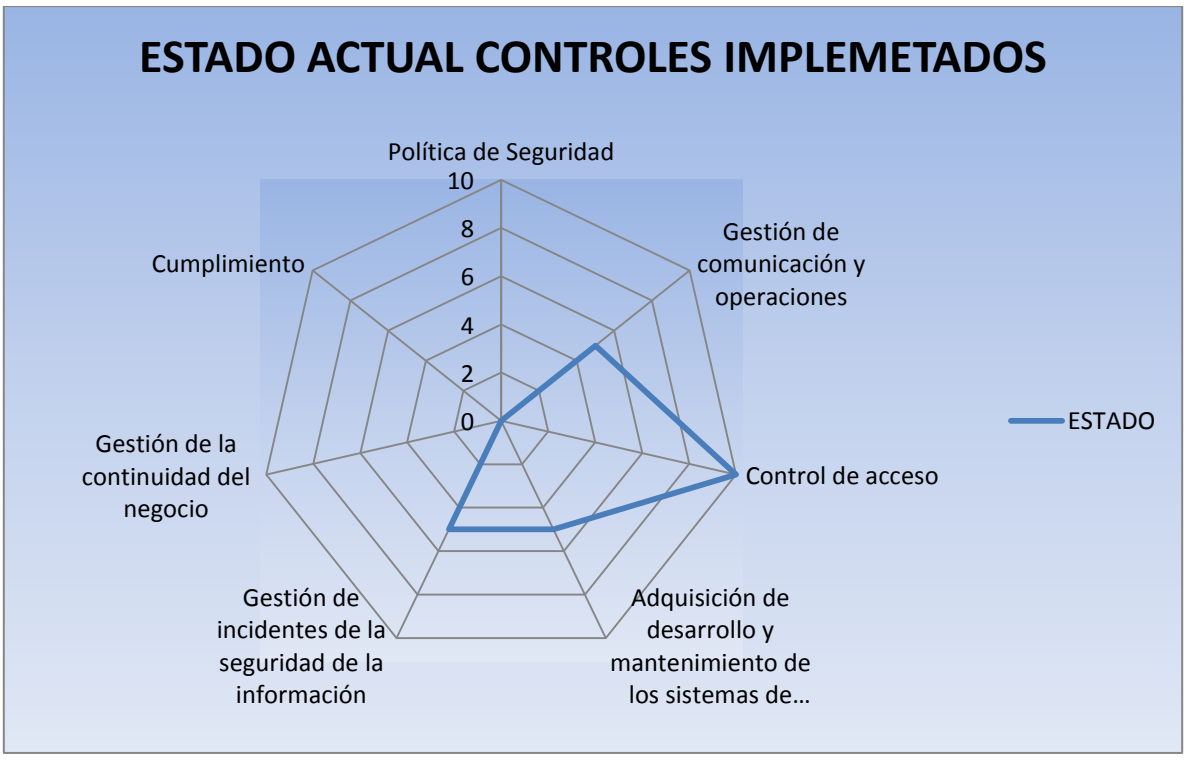
En el siguiente gráfico 1, obtenido de la tabla resumen del análisis diferencial, sobre el grupo de controles de la normativa ISO/IEC 27000 se ilustra el estado

actual de implementación de controles de seguridad de la información en la institución universitaria.

Tabla No. 3 Resumen análisis diferencial

CONTROLES DE SEGURIDAD	ESTADO
Política de Seguridad	0
Gestión de comunicación y operaciones	5
Control de acceso	10
Adquisición de desarrollo y mantenimiento de los sistemas de información	5
Gestión de incidentes de la seguridad de la información	5
Gestión de la continuidad del negocio	0
Cumplimiento	0

Gráfico No. 1 Estado análisis diferencial



1.3 Alcance

Teniendo en cuenta que la organización que se ha seleccionado para este proyecto de implementación de acuerdo a la normativa ISO/IEC 27001:2005 es una empresa mediana que posee procesos académicos y administrativos y presenta un nivel de seguridad bajo, es necesario empezar por las áreas o servicios que la empresa presta para cumplir su misión institucional, es decir, salvaguardar todos los sistemas de información que permiten dar un buen servicio a los estudiantes como clientes potenciales. En concreto, se debe implementar todos los controles de seguridad necesarios en todos los procesos académicos de la organización universitaria escogida más aún en los controles críticos que se evaluaron en el análisis diferencial reflejado en la tabla 2, anexada anteriormente. A continuación se relacionan el grupo de controles de la norma que son de carácter críticos en la empresa por no tenerlos implementados y marcan el nivel de seguridad actual de la empresa.

- Política de Seguridad
- Gestión de comunicación y operaciones
- Control de acceso
- Adquisición de desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

1.4 Plan director

Objetivos Generales

Elaborar el plan de implementación de Sistema de Gestión de la Seguridad de la Información bajo la ISO/IEC 27001:2005 del área académica de la universidad.

Objetivos específicos

- ✓ Analizar y conocer a fondo el grado de seguridad de información que actualmente posee la empresa
- ✓ Realizar planes de acción que permitan involucrar al personal encargado de la oficina de sistemas para todo el procesos de planeación para la implementación del SGSI

- ✓ Realizar el análisis de riesgos para la evaluación exahustiva de los activos que la empresa actualmente posee y la valoración de los mismos.
- ✓ Proponer las medidas correctoras planificadas para garantizar el nivel de seguridad más adecuado a las necesidades de la universidad.
- ✓ Definir los documentos que soportan los sistemas de seguridad de la organización
- ✓ Definir los planes de continuidad de negocio necesario para la preservación en caso de incidentes
- ✓ Determinar las amenazas a las que se encuentra expuesta la organización
- ✓ Definir los costos de inversión que aseguren la implentación del SGSI con todos los recursos físicos, lógicos y de personal necesario.
- ✓ Definir los planes de capacitación para la formación en el área de la seguridad informática al personal de la oficina de sistemas de la universidad.

2. FASE 2: SISTEMA DE GESTION DOCUMENTAL

En esta fase se relacionan todos los documentos que definen la ISO/IEC 27001 necesarios para certificar el sistema de gestión de seguridad implantados en la universidad. Cada documento se desarrolla en forma independiente, los cuales se relacionan y describen a continuación de manera resumida. .

✓ **Política de Seguridad:**

En este documento se especifica toda la normativa interna de la institución con el objetivo de que los funcionarios conozcan y cumplan sobre el sistema de gestión de la seguridad informática (SGSI) implantado. Así mismo contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que deben hace en caso de que ocurra un incidente de seguridad.

✓ **Gestión de roles y responsabilidades**

El SGSI, implantado en la institución se compone de un grupo que se encarga de crear, mantener, revisar , auditar y mejorar el sistema. Por lo tanto se hace necesario especificar en este documento los compromisos y responsabilidades que asume el equipo de trabajo que se estipula como comité de seguridad. En dicho comité hace parte por lo menos una persona de dirección para tener el respaldo de las directivas institucionales las decisiones que se requieran tomar.

✓ **Procedimientos de revisión por dirección**

La revisión por dirección es uno de los aspectos que contempla la normativa ISO/IEC 27001:2005 para la revisión anualmente de los aspectos más importantes que se han presentado con relación al SGSI implantados, revisando los elementos de entrada y salida de la revisión que establece la norma. De esta manera la dirección puede verificar y/o monitorear el sistema y establecer compromisos para realizar las mejoras necesarias.

✓ **Procedimientos de auditorías internas**

En este documento, se presenta toda la planificación de la auditoría que se debe realizar para mantener la vigencia de certificación obtenida en la implantación del SGSI de la institución. En dicho documento se establecen los requisitos que los auditores internos deben tener y se establece la forma como se presentará el informe de la auditoría.

- ✓ **Declaración de aplicabilidad**

En este documento se especifican todos los controles de seguridad que se establecieron en la organización y con el detalle de su aplicabilidad y descripción de cada uno.

Los anteriores documentos relacionados se anexan en archivos independientes en pdf.

3. FASE 3: METODOLOGIA DE ANALISIS DE RIESGOS

El análisis de riesgos es el proceso que determina el estado actual de la institución sobre la seguridad de la información. A través de este proceso se identifican las áreas que requieren medidas de protección. Para el caso de la institución el área identificada, es la parte académica teniendo en cuenta que es la razón de ser de la universidad y es su componente misional.

Esta fase se desarrolló en un documento independiente por cuanto la realización de este proceso es extensa y contiene elementos que se deben contemplar en forma independiente, ordenada y comprensible para la institución y verificación. Entre los componentes del documento se tiene el inventario de activos del área académica de la empresa, valoración de los activos, el análisis de las amenazas, la estimación del riesgo entre otras. El archivo que se adjunta también se encuentra en un formato en pdf.

4. FASE 4: PLAN DE TRATAMIENTO DE RIESGOS

En el plan de tratamiento de riesgos se indican todas las medidas de seguridad o controles que son necesarios para reducir los riesgos por cada activo, es decir todas las acciones que serán necesarias para implementar controles. Este plan de tratamiento también se estipula en un documento independiente en pdf.

5. FASE 5: AUDITORIA DE CUMPLIMIENTO

En esta fase se evalúa la madurez de la seguridad en los que corresponde a los diferentes dominios de control y los 133 controles planteados por la ISO/IEC 27002:2005 También se anexa en forma independiente en formato en pdf por su extensión y necesidad de especificación.

6. CONCLUSIONES

Implantar un Sistema de Gestión de la seguridad informática (SGSI) bajo la normativa ISO/IEC 27001:2005 en una organización real, permite en forma positiva identificar el estado en que se encuentran la seguridad los sistemas de información en las empresas y viviendo de primera mano la falta de conocimiento, sobre la necesidad de protección de la información como el activo más importante de las empresas y que ellas, aún no han ni siquiera estimado o contemplado los riesgos o perdidas económicas y los impactos que podrían tener si llegase a materializar una amenaza de seguridad a los sistemas de información que poseen para desarrollo de su actividad misional.

Otra de las conclusiones que se pueden presentar de este proyecto, es la experiencia y profundización que el estudiante obtiene al desarrollar cada uno de los elementos o aspectos que se deben realizar para una la implantación de un SGSI bajo la normativa ISO.

Es de anotar que realizar la implantación de un SGSI con éxito en una empresa, requiere tiempo, dedicación y compromiso tanto de los funcionarios como de las directivas de la empresa.

7. BIBLIOGRAFIA

Casanovas, Inés. Gestión de archivos electrónicos. , , Argentina: Alfagrama Ediciones, 2009. p 205. http://site.ebrary.com/lib/unadsp/Doc?id=10345376&ppg=205 Copyright © 2009. Alfagrama Ediciones. All rights reserved.

Seguridad Informática en Colombia. Tendencias 2008. Jeimy J. Cano, Ph.D, CFE

Gestión de la Seguridad Informática. Universidad Oberta de Catalunya. Daniel Cruz Allende.2007.

Casanovas, Inés. Gestión de archivos electrónicos. , , Argentina: Alfagrama Ediciones, 2009. p 205. http://site.ebrary.com/lib/unadsp/Doc?id=10345376&ppg=205 Copyright © 2009. Alfagrama Ediciones. All rights reserved.

Seguridad Informática en Colombia. Tendencias 2008. Jeimy J. Cano, Ph.D, CFE Coordinador Segurinfo
.
Seguridad de la Información ISO/IEC 27001. http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/

El portal de ISO 27001 en Español. http://www.iso27000.es/sgsi.html

Plan director de seguridad de la subdirección general de informática. http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&ved=0CDkQFjAC&url=http%3A%2F%2Fadministracionelectronica.gob.es%2Frecursos%2Fpae_000002763.pdf&ei=zJxDUZu2FNKz4AOI8oCQDw&usg=AFQjCNHUPTHPOKrzwC6dqg3dnoqZqvO97w